Benutzerhandbuch für Intego VirusBarrier X6

Willkommen beim Benutzerhandbuch für Intego VirusBarrier X6, dem besten Virenschutzprogramm für den Mac. Über das folgende Inhaltsverzeichnis können Sie die verschiedenen Abschnitte des Handbuchs öffnen. Sie können jederzeit zu diesem Hauptinhaltsverzeichnis zurückkehren, indem Sie auf den Link *Zum Hauptinhaltsverzeichnis wechseln* klicken, der sich oben auf jeder Seite befindet.

Informationen über die Installation von VirusBarrier X6 und die Aktualisierung des Programms und seiner Filter mit Intego NetUpdate finden Sie im Benutzerhandbuch für die ersten Schritte von Intego.

Inhaltsverzeichnis

1. Willkommen bei VirusBarrier X6
2. Erste Schritte mit Intego VirusBarrier X6
3. So schützen Sie Ihren Mac vor Viren und schädlicher Software
4. So schützen Sie Ihren Mac vor Netzwerkangriffen
5. So verwenden Sie die Überwachungstools von VirusBarrier X6
6. Einstellungen und Konfigurationen für VirusBarrier X6
7. Anhang: So erstellen Sie eigene Firewall-Regeln

© 2009 Intego. Alle Rechte vorbehalten.

Willkommen bei VirusBarrier X6

- Infos über Intego VirusBarrier X6
- Installation
- Aktualisierung von VirusBarrier X6 und Virusdefinitionen
- Infos über Ihre Kopie von Intego VirusBarrier X6
- Technische Kundenunterstützung

Zum Hauptinhaltsverzeichnis wechseln

Infos über Intego VirusBarrier X6

VirusBarrier X6 ist mehr als nur ein Virenschutzprogramm. Es ist das einzige Virenschutzprogramm für den Mac, das einen vollständigen Schutz vor schädlicher Software sowie eine Firewall und Funktionen zum Netzwerkschutz enthält. Kein anderes Virenschutzprogramm für den Mac enthält so viele Funktionen wie VirusBarrier X6.

Während Viren, trojanische Pferde, Würmer und andere Arten schädlicher Software eine ständige Bedrohung für alle Computer darstellen, wenden sich Cyber-Kriminelle neuen Techniken zu, um Ihren Mac zu infizieren und zu kontrollieren. Diese neuen Gefahren kommen leise und ohne große Vorwarnung über das Internet. In vielen Fällen kann nur der Besuch einer mit dieser versteckten Munition versehenen Website Ihren Mac gefährden. Es reicht nicht mehr aus, sich nur auf schädliche Software oder Netzwerk-Angriffe zu konzentrieren, um Macs vor den Gefahren aus dem Internet zu schützen. Daher hat sich Intego entschieden, die Funktionen seiner beiden anerkannten Programme – der Virenschutzanwendung VirusBarrier und der persönlichen Firewall NetBarrier – in eine einzige Anwendung zu integrieren. Diese wurde so optimiert, dass sie die zunehmenden kombinierten Angriffe verwalten kann.

VirusBarrier X6 ist die neueste Version des Intego-Sicherheitsprogramms für Netzwerke und schädliche Software, das die vielen Verteidigungsstrategien der früheren Versionen von VirusBarrier und NetBarrier enthält, mit denen Macs seit mehr als zehn Jahren geschützt wurden. Zusätzlich enthält es noch viele weitere Funktionen. VirusBarrier X6 schützt Macs durch verschiedene Techniken zur Gefahrenerkennung, verbesserte Erkennungsmethoden, kombinierte Erkennungsprotokolle, proaktive Verhaltensanalysen und die ganze Bandbreite an Verteidigungsfunktionen vor allen bekannten Netzwerk-basierten Gefahren sowie vor jeder bekannten schädlichen Software.

VirusBarrier X6 erkennt und entfernt:

- Mac-Viren

- Windows-Viren
- Unix-Viren
- Microsoft Word- und Excel-Makroviren
- Trojanische Pferde
- Würmer
- Spyware
- Adware
- Hacker-Tools
- Einwahlprogramme
- Keylogger
- Gefälschte Sicherheitsprogramme, auch "Scareware" genannt

Die Angriffe von Heute umfassen Trojanische Pferde, Cross-Site Scripting (XSS), Clickjacking, Phishing, vergiftetes JavaScript, schädliche Java-Applets und vieles mehr. Hacker erstellen Viren nicht mehr nur für den Nervenkitzel, wenn sie sehen, wie Computer infiziert werden. Cyber-Kriminelle machen das für Geld und nutzen ihre Angriffe, um die DNS-Einstellungen infizierter Macs zu kapern und sie so an betrügerische Websites zu senden sowie die Passwörter und Kreditkartennummern abzugrasen. Sie erstellen Botnets (Netzwerke von infizierten Computern), die auf ihre Befehle reagieren, um auf diese Weise Spam zu verschicken oder andere Computer anzugreifen. Sie installieren Rootkits (Administratorenbausätze), um einen Zugriff aus der Ferne auf einen infizierten Computer herzustellen. So können sie Passwörter und andere persönliche Informationen stehlen. Oder sie erstellen Exploits, um Schwachstellen in Mac OS X auszunutzen oder in bestimmter Software, die verwendet wird (Flash Player, QuickTime, PHP, Apache etc.) und übernehmen so die Kontrolle über Ihren Mac.

VirusBarrier X6 schützt Macs vor Netzwerk-Eindringversuchen, indem alle über das Internet oder ein anderes Netzwerk ein- und alle ausgehenden Datenpakete kontinuierlich gefiltert werden. Mit VirusBarrier X6 sind Macs vor Datendiebstahl, Hackerangriffen und Eindringversuchen geschützt. Die Software warnt Benutzer automatisch bei verdächtigen Aktivitäten.

VirusBarrier X6 schützt Macs vor:

- Eindringversuchen über das Netzwerk
- DoS-Angriffen
- Janusangriffen
- Ping-Überflutung
- Port-Scans
- Cross-Site Scripting-Angriffen (XSS)
- Heimliches Herunterladen von Software
- Phishing
- Clickjacking
- Webseiten mit schädlichem JavaScript
- Schädlichen Java-Applets
- Rootkits (Administratorbaukästen)

Durch die Kombination der Funktionen von VirusBarrier und NetBarrier in einem einzigen Programm sorgt Intego dafür, dass Mac-Benutzer sich leichter vor jeder Art von Gefahr oder Angriff schützen können.

Installation

Systemanforderungen

Jeder offiziell unterstützte Mac OS X-kompatible Computer
- Mac OS X 10.5 oder neuer, VirusBarrier X6 ist voll kompatibel mit Mac OS X 10.6 Snow Leopard und Mac OS X 10.5 Leopard. VirusBarrier X6 wird nicht für die Verwendung unter Mac OS X Server unterstützt.
- 100 MB freier Festplattenspeicherplatz

Installation von Intego VirusBarrier X6

Informationen über die Installation und Registrierung von Intego VirusBarrier X6 erhalten Sie im Intego-Handbuch für die ersten Schritte.

Aktualisierung von VirusBarrier X6 und Virusdefinitionen

Intego VirusBarrier X6 verwendet die mit dem Programm installierte Anwendung Intego NetUpdate, um Aktualisierungen für die Filter und Virusdefinitionen des Programms sowie auch für das Programm selbst zur Verfügung zu stellen. Weitere Informationen über die Verwendung von NetUpdate finden Sie im Intego-Handbuch für die ersten Schritte.

Infos über Ihre Kopie von Intego VirusBarrier X6

Wenn Sie Informationen über Ihre Kopie von VirusBarrier X6 erhalten möchten, wählen Sie "VirusBarrier X6 > Über VirusBarrier X6". Sie erhalten Informationen über Intego VirusBarrier X6, wie beispielsweise die Versionsnummer, Ihre Kundendienstnummer (die Sie benötigen, wenn Sie technische Kundenunterstützung anfordern) und einen anklickbaren Link, um eine E-Mail an die Kundenunterstützungsabteilung von Intego zu senden.

Technische Kundenunterstützung

Als registrierter Kunde von Intego mit gültigen Abonnements erhalten Sie von Intego technische Kundenunterstützung auf der Intego Support-Seite.

© 2009 Intego. Alle Rechte vorbehalten.

Erste Schritte mit Intego VirusBarrier X6

- So verwenden Sie den Konfigurationsassistenten
- So verwenden Sie das Übersichtsfenster von VirusBarrier X6
- Statusanzeigen im Übersichtsfenster
- Scannen schädlicher Software auf einen Blick
- So verwenden Sie das Intego-Menü

Zum Hauptinhaltsverzeichnis wechseln

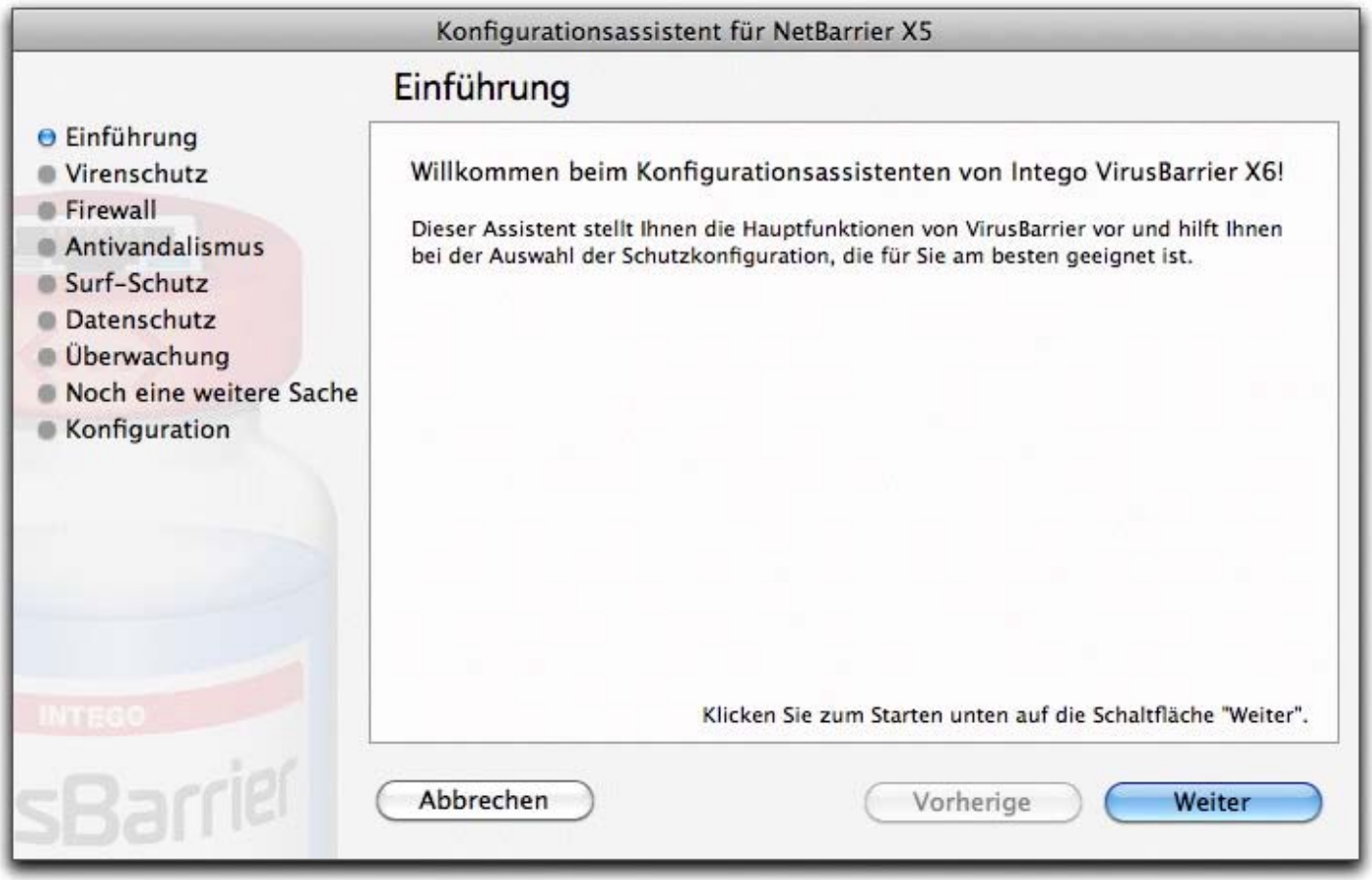
Wenn Sie VirusBarrier X6 das erste Mal starten, müssen Sie auswählen, wie das Programm konfiguriert werden soll, damit es Ihnen einen optimalen Schutz für die Art bieten kann, wie Sie Ihren Mac verwenden. VirusBarrier X6 enthält einen Konfigurationsassistenten, der Ihnen dabei hilft. Zudem erklärt er Ihnen die vielen Funktionen zum Netzwerkschutz und zum Schutz vor schädlicher Software, die das Programm bietet.

So verwenden Sie den Konfigurationsassistenten

Der Konfigurationsassistent von VirusBarrier X6 hilft Ihnen, die grundlegenden Einstellungen des Programms schnell und einfach anzupassen, damit sie zu der Art und Weise passen, wie Sie Ihren Mac verwenden. Wenn Sie VirusBarrier X6 zum ersten Mal öffnen, wird der Konfigurationsassistent automatisch gestartet.

Wenn Sie den Konfigurationsassistenten irgendwann einmal manuell starten möchten, wählen Sie einfach VirusBarrier X6 > Einstellungen, klicken Sie auf das Symbol "Erweitert" und dann auf "Assistenten anzeigen...". Um den Konfigurationsassistenten ausführen zu können, benötigen Sie ein Administratorkennwort.

Hinweis: Wenn Sie von einer früheren Version von VirusBarrier oder NetBarrier aktualisiert haben, übernimmt das Programm die Einstellungen, die Sie in diesen Programmen festgelegt haben. Wenn Sie beide Programme hatten, werden alle Einstellungen importiert. Wenn Sie jedoch nur eines der beiden Programme hatten und den Konfigurationsassistenten ausführen, überschreibt VirusBarrier X6 die vorhandenen Einstellungen. In diesem Fall sollten Sie den Assistenten eventuell schließen und die Einstellungen für den Netzwerkschutz und den Schutz vor schädlicher Software manuell einstellen.



Die ersten acht Fenster des Konfigurationsassistenten von VirusBarrier X6 zeigen kurz Informationen über die

verschiedenen Funktionen des Programms an:

- **Virenschutz**
- **Firewall** (Regeln und Trojanische Pferde)
- **Antivandalismus** (Richtlinie, Gesperrte Adressen und Vertrauenswürdige Adressen)
- **Surf-Schutz**
- **Datenschutz** (Anti-Spyware, Daten)
- **Überwachung** (Überwachungstools)
- **Noch eine weitere Sache** (verschiedene Funktionen)

Wenn Sie fertig sind, können Sie im Konfigurationsfenster auswählen, welche Konfiguration von VirusBarrier X6 Sie verwenden möchten.

Dabei handelt es sich um folgende Konfigurationen:

Name	Am besten wenn...	Einstellungen für Netzwerkschutz und Schutz vor schädlicher Software	Andere Einstellungen
Einfach	...Sie einen Zugriff auf Ihren Mac von einem lokalen Netzwerk zulassen müssen, aber vor Eindringversuchen von außerhalb	Der Echtzeit-Scanner ist aktiv, um Sie vor schädlicher Software zu schützen. Die Firewall ist auf den Modus "Client, lokaler Server" eingestellt: Ihr Mac kann als Client-Computer auf das Internet zugreifen und Ihr Mac kann sowohl als Client als auch als Server in einem lokalen Netzwerk dienen.	Antivandalismusfilter sind gegen Pufferüberlauf-Angriffe, Eindringversuche, Ping-Angriffe, Port-Scans und SYN-Flooding aktiviert. Für Ping-Übertragungen sind sie hingegen deaktiviert. Anti-Phishing-

	Ihres lokalen Netzwerks geschützt sein möchten.	Die Suche nach schädlicher Software für Windows und Linux ist deaktiviert und die Suche nach schädlicher Software in Archiven ist deaktiviert.	Schutz ist aktiviert. Web Threat-Schutz ist deaktiviert. Datenschutzfilter sind deaktiviert.
Standard	...Sie Ihren Computer nicht als Netzwerkserver oder für das lokale Filesharing verwenden.	Der Echtzeit-Scanner ist aktiv, um Sie vor schädlicher Software zu schützen. Die Firewall ist auf den Modus "Client, lokaler Server" eingestellt: Ihr Mac kann als Client-Computer auf das Internet zugreifen und Ihr Mac kann sowohl als Client als auch als Server in einem lokalen Netzwerk dienen. Die Suche nach schädlicher Software für Windows und Linux ist aktiviert, ebenso die Suche nach schädlicher Software in Archiven.	Antivandalismusfilter sind gegen Pufferüberlauf-Angriffe, Eindringversuche, Ping-Angriffe, Port-Scans und SYN-Flooding aktiviert. Für Ping-Übertragungen sind sie hingegen deaktiviert. Anti-Phishing-Schutz ist aktiviert. Web Threat-Schutz ist aktiviert. Datenschutzfilter sind deaktiviert.
Stark	...Sie maximalen Schutz wünschen und akzeptieren können, dass diese Konfigurationen einigen Datenverkehr sperren kann.	Der Echtzeit-Scanner ist aktiv, um Sie vor schädlicher Software zu schützen. Die Firewall ist auf den Modus "Nur Client" eingestellt: Ihr Mac funktioniert nur als Client in einem lokalen Netzwerk oder im Internet. Die Server-Funktionen Ihres Computers sind gesperrt.	Alle Antivandalismus-Filter sind deaktiviert, wie beispielsweise die, die vor Trojanischen Pferden schützen. Anti-Phishing-Schutz ist aktiviert. Web Threat-Schutz ist aktiviert. Datenschutzfilter sind aktiviert.

Nachdem Sie Ihre Schutzstufe ausgewählt haben, können Sie sofort eine vollständige Suche nach Viren und schädlicher Software auf Ihrem Mac durchführen lassen. So gehen Sie sicher, dass sich auf Ihrem Mac keine schädliche Software befindet bzw. schädliche Software wird aufgespürt und entfernt. Wenn Sie diese Aktion durchführen möchten, lassen Sie das Kontrollkästchen "Nach der Konfiguration eine vollständige Virensuche durchführen" markiert. Sie können diese Virensuche auch später manuell durchführen. Deaktivieren Sie diese Option in diesem Fall. Weiter hinten in diesem Kapitel erhalten Sie eine Einführung, wie Sie Ihren Mac nach Viren und schädlicher Software durchsuchen. Detaillierte Informationen über die Suche nach schädlicher Software auf Ihrem Mac erhalten Sie auch unter So schützen Sie Ihren Mac vor Viren und schädlicher Software.

Klicken Sie auf die Schaltfläche "Konfigurieren", um die ausgewählte Konfiguration auszuwählen und eine vollständige Suche nach Viren und schädlicher Software durchführen zu lassen (sofern Sie diese Option ausgewählt haben).

So verwenden Sie das Übersichtsfenster von VirusBarrier X6

Wenn Sie VirusBarrier X6 öffnen, wird das Übersichtsfenster angezeigt. Dieses Fenster zeigt Informationen darüber an, wie VirusBarrier X6 läuft und bietet eine Rückmeldung der Programmaktivitäten in Echtzeit.

Über das Übersichtsfenster erhalten Sie einen schnellen Zugriff auf:

- Die Funktionen, Einstellungen und Protokolle von VirusBarrier X6,
- mehrere hilfreiche Netzwerkdienstprogramme (z.B. Whois und Traceroute),
- grafische Anzeigen der aktivierten Schutzarten,
- Informationen über das Programm selbst (z.B. wann es zuletzt aktualisiert wurde),
- eine Möglichkeit mehrere Konfigurationen zu verwalten, damit Sie die Schutzeinstellungen schnell ändern können.

Am oberen Rand des Übersichtsfensters gibt es eine Zeile mit Schaltflächen, über die Sie Zugriff auf die vielen Einstellungen von VirusBarrier X6 erhalten. Die vier Schaltflächen ganz links führen zu den Einstellungen, die festlegen, wie VirusBarrier Sie gegen schädliche Software schützt. Einzelheiten zu diesen Einstellungen erhalten Sie unter So schützen Sie Ihren Mac vor Viren und schädlicher Software.

Die vier Schaltflächen ganz rechts führen zu den Bedienelementen für den Netzwerkschutz. Einzelheiten zu diesen Einstellungen erhalten Sie unter So schützen Sie Ihren Mac vor Netzwerkangriffen.

Wenn Sie auf die Schaltflächen für den Schutz vor schädlicher Software oder den Netzwerkschutz klicken, werden Fenster mit Registerkarten geöffnet, die zu weiteren Bedienelementen führen. Wenn Sie auf die Schaltfläche "Firewall" klicken wird beispielsweise ein Fenster mit zwei Registerkarten geöffnet: "Firewall-Regeln" und "Trojaner".

Die mittlere Schaltfläche in dieser Zeile führt zurück zum Übersichtsfenster.

Jede dieser Schaltflächen leuchtet grün auf, wenn das zugehörige Fenster aktiv ist.

Die kleineren Schaltflächen in der unteren rechten Ecke sind die Bedienelemente für die Überwachung.

Sie können auf die Überwachungsfunktionen auch über die Auswahl im Menü "Ansicht" oder mithilfe von Tastenkombinationen zugreifen. Dabei handelt es sich um Folgende:

	Protokoll	Wahltaste-Befehlstaste-L	Zeigt eine Aufzeichnung der Aktivitäten von VirusBarrier und des Datenverkehrs an, der von Ihrem Mac ins Internet oder in lokale Netzwerke abgeht oder von dort empfangen wird.
	Dienste	Wahltaste-Befehlstaste-1	Zeigt eine Liste der Wege an, auf denen Ihr Mac Informationen an die Außenwelt liefern kann.
	Traceroute	Wahltaste-Befehlstaste-2	Zeigt den Netzwerkpfad an, den ein Signal nimmt, um von Ihrem Mac zu einem anderen Computer zu gelangen.

	Whois	Wahltaste-Befehlstaste-3	Zeigt Informationen über die Eigentümer und Verwalter von Internetdomänen an.
	Datenverkehr	Wahltaste-Befehlstaste-4	Zeigt den ein- und ausgehenden Netzwerkverkehr auf Ihrem Mac an.
	Netzwerke	Wahltaste-Befehlstaste-5	Zeigt Außen-Netzwerke an, die derzeit für Ihren Mac zur Verfügung stehen.

Jede dieser Funktionen wird unter So verwenden Sie die Überwachungstools von VirusBarrier X6 beschrieben.

In der unteren linken Ecke gibt es eine Schaltfläche, mit der Sie sich eine Liste der Konfigurationen anzeigen lassen können. (Sie können auch zwischen dem Ein- und Ausblenden der Konfigurationsliste hin- und herwechseln, indem Sie Befehlstaste-K drücken oder "Ansicht > Konfigurationen anzeigen/verbergen" wählen.)

Jede Konfiguration besteht aus einer Sammlung von Einstellungen für den Schutz vor schädlicher Software und den Netzwerkschutz von VirusBarrier X6. Zu Beginn gibt es nur eine Konfiguration. Entweder trägt diese den Namen, den Sie im Konfigurationsassistenten gewählt haben, oder sie heißt "Standard" (falls Sie den Assistenten nicht ausgeführt haben). Das runde Optionsfeld zeigt an, welche Konfiguration gerade aktiv ist.

Am unteren Rand der Konfigurationsliste befindet sich eine Aktionsschaltfläche, mit der Sie die Konfigurationen duplizieren, bearbeiten und entfernen können. Weitere Informationen finden Sie unter Einstellungen und Konfigurationen für VirusBarrier X6.

Neben der Konfigurationsschaltfläche gibt es eine Schaltfläche zum Sperren, mit der Sie VirusBarrier X6 sperren können, damit andere Benutzer die Programmeinstellungen nicht verändern können. Da Benutzer, die nicht über ein Administratorkonto verfügen, keine Änderungen an den Einstellungen von VirusBarrier X6 vornehmen können, müssen Administratoren das Programm entsperren, um Änderungen daran vorzunehmen. Sie können auf die Schaltfläche zum Sperren klicken, um den Zugriff auf die Einstellungen wieder zu sperren. (Nicht-Administratoren haben Zugriff auf alle VirusBarrier X6-Funktionen zum Scannen und Überwachen).

Wenn Sie VirusBarrier X6 sperren möchten, klicken Sie entweder auf die Schaltfläche zum Sperren, auf "Befehlstaste-L" oder wählen Sie "Ablage > Einstellungen sperren". Wenn Sie VirusBarrier X6 entsperren möchten, klicken Sie noch einmal auf das Schlosssymbol, drücken Sie Befehlstaste-L oder wählen Sie "Ablage > Einstellungen entsperren". Geben Sie dann Ihr Administratorpasswort ein, um den Vorgang abzuschließen.

Am obersten Rand des Übersichtsfensters befindet sich die Statusleiste von NetUpdate. Sie zeigt an, wann die neuesten VirusBarrier-Filter auf Ihrem Mac installiert wurden und ob Ihre Filter aktualisiert werden müssen. Zudem zeigt sie an, wie lange Ihr Abonnement noch gültig ist. VirusBarrier X6 verwendet Intego-NetUpdate, um regelmäßig nach Aktualisierungen zu suchen. Sie können auch manuell nach Aktualisierungen suchen, indem Sie auf "Jetzt prüfen" in der oberen rechten Ecke klicken. Wenn Sie die Statusleiste von NetUpdate ausblenden möchten, wählen Sie "Ansicht > Statusleiste für NetUpdate ausblenden". Weitere Informationen über die Verwendung von NetUpdate finden Sie im Benutzerhandbuch von Intego für die ersten Schritte.

VirusBarrier X6
Ihre Filter sind auf dem aktuellen Stand. Installierte Filter: 12.12.2009
Ihr Abonnement läuft in 12 Monaten aus
Jetzt prüfen

Statusanzeigen im Übersichtsfenster

Der Status vieler VirusBarrier X6-Funktionen wird im Übersichtsfenster angezeigt. Die Anzeigen für den Schutz vor schädlicher Software befinden sich auf der linken Fensterseite.

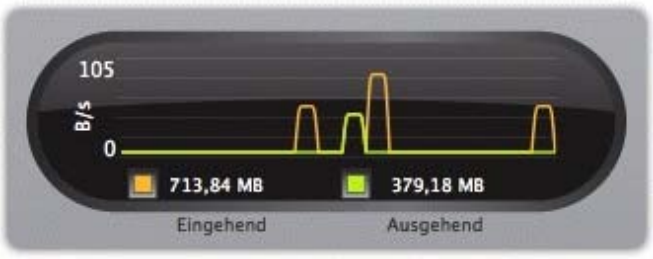
Die Anzeigen für den Netzwerkschutz befinden sich auf der rechten Seite.

Wenn Sie auf eine der Anzeigen klicken, wird ein Fenster geöffnet, in dem Sie die Einstellungen für diese Anzeige überprüfen und ändern können.

Die Anzeigen für den Anti-Phishing- und Web Threat-Schutz leuchten grün, wenn sie aktiviert sind (siehe Abbildung oben). Wenn sie deaktiviert sind, leuchten sie grau.

Unten links im Fenster gibt es zwei Messskalen, die die aktuellen und vergangenen Aktivitäten des Echzeit-Scanners anzeigen. Dieser überwacht Ihren Mac kontinuierlich und sucht nach Infektionen durch schädliche Software.

Im Bereich unten rechts des Fensters wird der aktuelle Netzwerk-Datendurchsatz angezeigt (sowohl ein- als auch ausgehender Datenverkehr).



Scannen schädlicher Software auf einen Blick

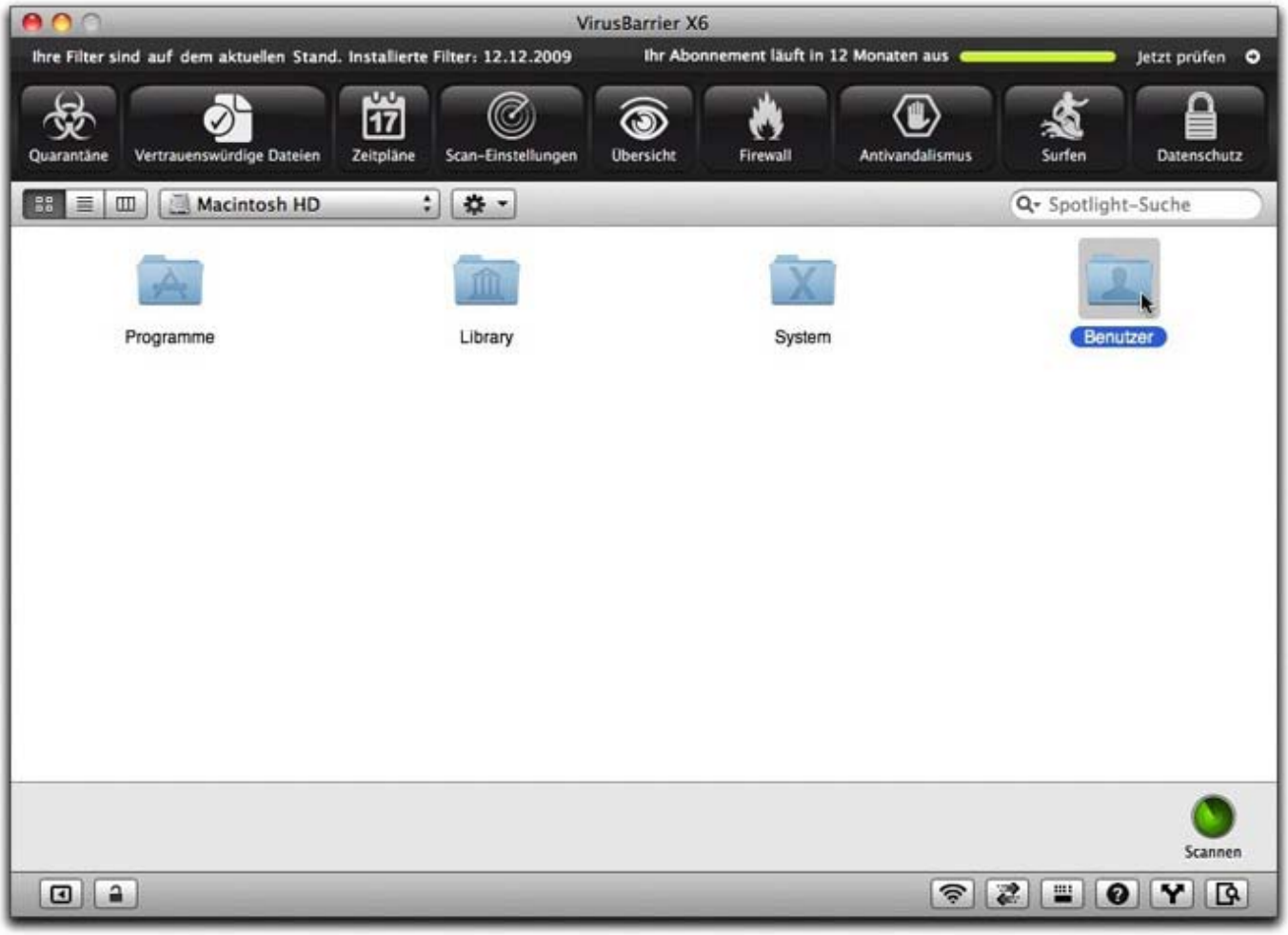
Sie können Ihren Mac automatisch von VirusBarrier X6 nach schädlicher Software durchsuchen lassen, nachdem Sie Ihre Schutzstufe im Konfigurationsassistenten ausgewählt haben. Der Echtzeit-Scanner von VirusBarrier X6 überwacht Ihren Computer im Anschluss weiter, um mögliche Infektionen zu verhindern. Sie können aber jederzeit auch eine manuelle Suche nach schädlicher Software durchführen. Alle Einzelheiten dazu erfahren Sie unter So schützen Sie Ihren Mac vor Viren und schädlicher Software. Hier aber einige Tipps, damit Sie schnell loslegen können.

Wenn Sie Ihren gesamten Mac und alle angeschlossenen Datenträger scannen möchten, klicken Sie einfach auf die Schaltfläche "Vollständiger Scan".

Wenn Sie schnell bestimmte Dateien oder Ordner scannen möchten, ziehen Sie diese einfach auf das Programmsymbol im Finder oder im Dock und legen Sie sie dort ab. Oder ziehen Sie sie auf die Kugel, wenn VirusBarrier X6 gerade ausgeführt wird.

Wenn Sie nur ausgewählte Dateien oder Laufwerke mithilfe der Oberfläche von VirusBarrier X6 scannen möchten, klicken Sie auf die Schaltfläche "Auswählen". Daraufhin werden Ihnen alle Festplatten, Laufwerke oder andere Speichermedien angezeigt, die mit Ihrem Mac verbunden sind.

Navigieren Sie dann wie im Finder zu der Datei, dem Ordner oder dem Laufwerk, die, den oder das Sie scannen lassen möchten. Klicken Sie zur Auswahl auf das Objekt oder drücken Sie auf die Befehlstaste, während Sie klicken, um mehrere Objekte auszuwählen. Klicken Sie anschließend auf die Schaltfläche "Scannen".



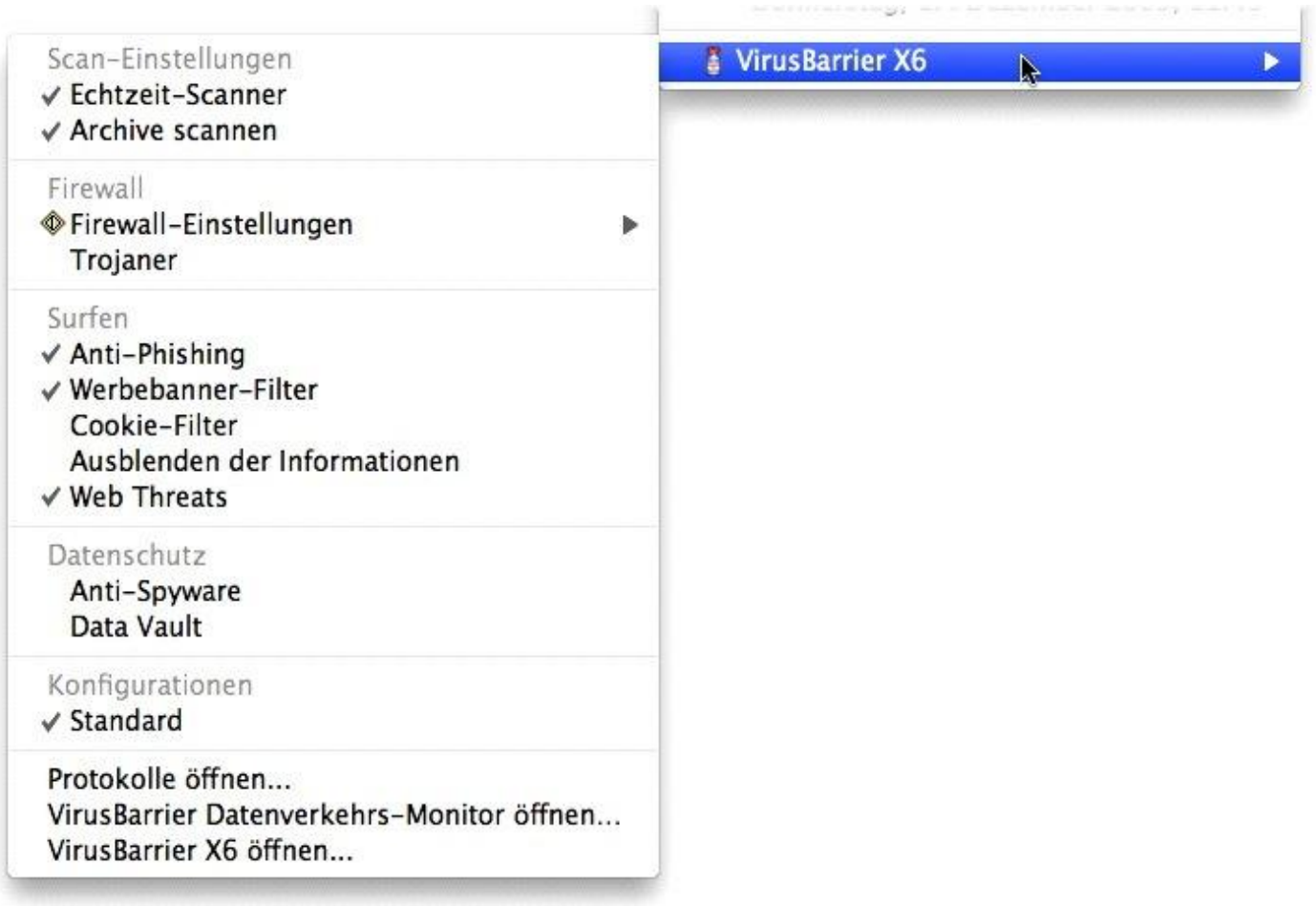
VirusBarrier X6 informiert Sie, wenn Dateien gefunden werden, die durch irgendeine bekannte schädliche Software infiziert wurden. Weitere Informationen über Warnmeldungen von VirusBarrier X6 und ihre Bedeutung erhalten Sie unter So schützen Sie Ihren Mac vor Viren und schädlicher Software.

So verwenden Sie das Intego-Menü

VirusBarrier X6 installiert ein Menü namens Intego-Menü in der Menüleiste. Das Symbol dieses Menüs ist der kleine Turm aus dem Intego-Logo.

Wenn Sie auf das Intego-Menü klicken, wird Ihnen ein Menü mit der gesamten, auf Ihrem Computer installierten Intego-Software angezeigt:

Aus dem Intego-Menü können Sie viele Einstellungen von VirusBarrier X6 ändern. Wählen Sie das Intego-Menü > VirusBarrier X6. Sie können den Echtzeit-Scanner starten und anhalten, Sie können Konfigurationen ändern und Sie können Einstellungen ein- und ausschalten, wie z.B. die Einstellungen für das Surfen oder den Datenschutz. Sie können auch den VirusBarrier Traffic Monitor öffnen, indem Sie das entsprechende Menüelement am unteren Rand des Menüs auswählen.



Weitere Informationen über diese Funktionen erhalten Sie in den jeweiligen Abschnitten dieses Handbuchs: So schützen Sie Ihren Mac vor Viren und schädlicher Software und So schützen Sie Ihren Mac vor Netzwerkangriffen.

© 2009 Intego. Alle Rechte vorbehalten.

So schützen Sie Ihren Mac vor Viren und schädlicher Software

- Ausführen manueller Scanvorgänge
- Warnmeldungen bei schädlicher Software
- Scan-Einstellungen
- Vertrauenswürdige Dateien
- Quarantänezone
- Das Kontextmenü für VirusBarrier X6
- Verwenden von VirusBarrier X6 über die Befehlszeile
- Verwenden von VirusBarrier X6 und AppleScript

Zum Hauptinhaltsverzeichnis wechseln

VirusBarrier X6 schützt auf verschiedene Arten vor schädlicher Software. Der Echtzeit-Scanner überwacht Ihren Mac kontinuierlich und schützt Sie so vor Viren und schädlicher Software. Der Echtzeit-Scanner stellt sicher, dass Ihr Mac jederzeit geschützt ist. Hierzu wird jede erstellte, kopierte, geänderte oder gesicherte Datei gescannt. Andere Dateien werden jedoch nicht gescannt. Deshalb empfehlen wir, dass Sie nach der Installation von VirusBarrier X6 und nach jeder Aktualisierung der Virusdefinitionen des Programms einen vollständigen Scanvorgang für Ihre Dateien ausführen.

Sie können auch den Scanner auf Abruf von VirusBarrier X6 verwenden, um Dateien, Ordner, Festplatten oder Datenträger auf Ihrem Mac zu überprüfen.

Ausführen manueller Scanvorgänge

Sie können jederzeit einen manuellen Scanvorgang mit VirusBarrier X6 starten. Sie sollten sofort nach der Installation einen Scanvorgang durchführen, damit sich auf keinen Fall infizierte Dateien auf Ihrem Computer befinden. Im Konfigurationsassistenten von VirusBarrier X6 können Sie festlegen, dass nach der ersten Einrichtung des Programms ein Scanvorgang durchgeführt werden soll. Anschließend sorgt der Echtzeit-Scanner von VirusBarrier X6 dafür, dass neue Dateien, die Sie Ihrem Mac hinzufügen, sicher sind.

Wenn Sie schnell einzelne Dateien oder Ordner scannen möchten, ziehen Sie diese einfach auf das Programmsymbol im Finder oder im Dock und legen Sie sie dort ab. Oder ziehen Sie sie auf die Kugel, wenn VirusBarrier X6 gerade ausgeführt wird.

Wenn VirusBarrier X6 ausgeführt wird, können Sie weitere Scanmöglichkeiten auswählen. Klicken Sie zuerst auf die Schaltfläche "Auswählen", damit Ihnen alle Festplatten, Laufwerke und anderen Speichermedien angezeigt werden, die mit Ihrem Mac verbunden sind.

Wie im Finder werden Ihnen Ordner und Dateien auf einem Laufwerk angezeigt, die Sie auswählen können, indem Sie darauf doppelklicken. Sie können auch die Darstellung ändern, damit Ihnen die Dateien in einer einfachen Liste oder in einem Dateibrowser angezeigt werden. Klicken Sie hierzu auf die Schaltflächen für die Darstellung in der oberen linken Ecke des Fensters.

In der Listenansicht können Sie sich Dateien innerhalb eines Ordners anzeigen lassen, indem Sie links vom Ordnernamen auf das dazugehörige Schließdreieck klicken.

Unabhängig von der Darstellungsart Ihrer Dateien können Sie mehrere Objekte auswählen, indem Sie die Befehlstaste gedrückt halten, während Sie nacheinander auf die Objekte klicken. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf die Schaltflächen "Scannen" in der unteren rechten Ecke, um den Vorgang zu starten.

Standardmäßig zählt VirusBarrier X6 zuerst die Anzahl der zu scannenden Dateien. Während des Scanvorgangs werden dann die Anzahl der bereits gescannten Dateien angezeigt und wieviel Prozent des Scanvorgangs bereits abgeschlossen sind.

VirusBarrier X6 kann Dateien scannen, die in komprimierten Archiven enthalten sind. Beim Scannen von Archiven ändert sich die Anzeige der Kugel und gibt an, dass ein Archiv bearbeitet wird. Sie haben die Möglichkeit, das Scannen dieses Archivs zu überspringen, wenn es sehr groß ist und sich sicher sind, dass es keine Viren enthält.

Beim Durchsuchen eines iPhones oder iPod touch kopiert VirusBarrier X6 alle Dateien vom Gerät auf das Startvolumen des Benutzers, um die Sicherheit zu überprüfen. Wenn schädliche Software oder infizierte Dateien gefunden werden, benachrichtigt VirusBarrier X6 den Benutzer und bietet an, die infizierten Dateien zu reparieren oder zu löschen.

Sie können den Scanvorgang jederzeit stoppen, indem Sie auf die Schaltfläche "Stoppen" klicken. Wenn Sie den Scanvorgang vorübergehend anhalten möchten, halten Sie die Wahltaste auf Ihrer Tastatur gedrückt und klicken Sie auf diese Schaltfläche, die jetzt die Bezeichnung "Pause".

Sie können die Virensuche fortsetzen, indem Sie auf die gleiche Schaltfläche klicken, die nun mit "Fortfahren" beschriftet ist.

Bei einem manuellen Scanvorgang werden Sie von VirusBarrier X6 darüber informiert, wenn Dateien gefunden werden, die mit schädlicher Software infiziert sind. Wenn VirusBarrier X6 eine mit einem Virus infizierte Datei gefunden hat, wird die Kugel für die funktionsabhängige Bedienung rot. Wenn VirusBarrier X6 beschädigte Dateien erkennt, wird die Kugel orange. Wenn sowohl mit einem Virus infizierte als auch beschädigte Dateien gefunden werden, blinkt die Kugel für die funktionsabhängige Bedienung rot und orange. VirusBarrier X6 alarmiert Sie entsprechend der vorgenommenen Einstellungen. Weitere Warnmeldungsoptionen finden Sie unter Einstellungen und Konfigurationen für VirusBarrier X6.

Schnelle Scanvorgänge

Mit VirusBarrier X6 können Sie schnelle Scanvorgänge ausführen, bei denen nur die Speicherorte überprüft werden, an denen schädliche Software normalerweise installiert wird. Wenn neue schädliche Software auftaucht, können Sie die gescannten Dateien und Ordner ändern. Zudem können mit neueren Versionen der Virusdefinitionen von VirusBarrier X6 eventuell andere Speicherorte gescannt werden.

Wenn Sie einen schnellen Scanvorgang ausführen möchten, klicken Sie auf die Schaltfläche "Übersicht" im VirusBarrier X6-Fenster, wenn die Kugel nicht sichtbar ist. Halten Sie die Wahltaste gedrückt. Sie werden dann sehen, dass sich die Schaltfläche "Vollständiger Scan" in die Schaltfläche "Schneller Scan" verwandelt. Klicken Sie auf diese Schaltfläche, um einen schnellen Scanvorgang zu starten.

Scanvorgang per Drag&Drop

Sie können jeden Datenträger, Ordner und jede Datei scannen, indem Sie ihn/sie einfach bei gedrückter Maustaste mit dem Cursor auf die Kugel ziehen. Sie müssen eventuell das Administratorpasswort eingeben, wenn Sie nicht die entsprechenden Rechte für den Zugriff auf Dateien haben, die in dem Objekt enthalten sind, das Sie auf die Kugel ziehen.

Sie können Datenträger, Ordner und Dateien hierzu auch einfach auf das Programmsymbol von VirusBarrier X6 im

Finder ziehen.

Sie können zu scannende Objekte auf die gleiche Weise auch auf das Symbol von VirusBarrier X6 im Dock ziehen.

Wenn Sie das jeweilige Symbol loslassen, wird das entsprechende Objekt auf die gleiche Weise wie beim manuellen Starten des Scanvorgangs nach schädlicher Software durchsucht.

Ausführen von Scanvorgängen aus dem Menü "Ablage"

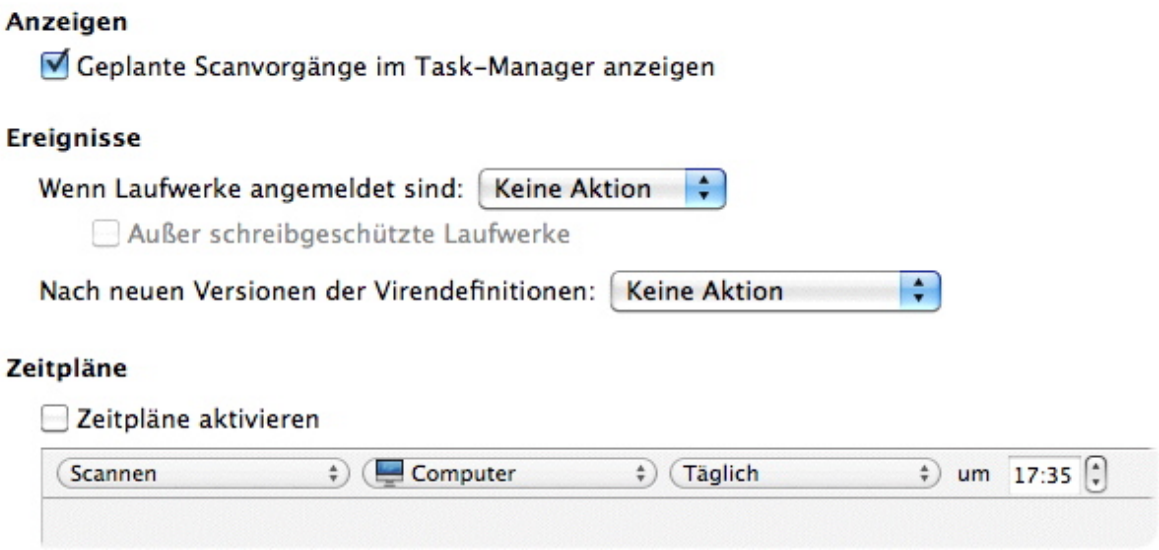
Sie können Scanvorgänge aus dem Menü "Ablage" von VirusBarrier X6 durchführen. Sie können "Scannen" auswählen (oder Befehlstaste-O drücken), um den Browser zu öffnen und Objekte zum Scannen auszuwählen. Sie können auch einen vollständigen Scanvorgang ausführen, indem Sie "Vollständiger Scan" wählen oder "Befehlstaste-S" drücken. Oder Sie führen einen schnellen Scanvorgang aus, indem Sie "Schneller Scan" auswählen oder "Befehlstaste-Wahltaste-S" drücken. Diese Scanvorgänge werden auf die gleiche Weise ausgeführt, wie die zuvor beschriebenen manuell gestarteten Scanvorgänge.

Geplante Scanvorgänge

VirusBarrier X6 kann auch so eingestellt werden, dass es zu zuvor festgelegten Zeitpunkten ausgeführt wird. Klicken Sie hierzu auf die Schaltfläche "Zeitpläne" am oberen Fensterrand.

Oder klicken Sie auf die Schaltfläche "Zeitpläne" im Übersichtsfenster von VirusBarrier X6.

In beiden Fällen wird das Fenster "Zeitpläne" angezeigt. Darin gibt es drei Abschnitte: "Anzeigen", "Ereignisse" und "Zeitpläne".



Im Abschnitt "Anzeigen" gibt es nur ein Kontrollkästchen: **Geplante Scanvorgänge im Task-Manager anzeigen**. Wenn dieses Kontrollkästchen aktiviert ist, wird ein kleines Fenster angezeigt, wenn auf Ihrem Mac geplante Scanvorgänge ausgeführt werden. Ist das Kontrollkästchen nicht aktiviert, werden Sie bei solchen Scanvorgängen nicht benachrichtigt (außer bei einem Virusfund).

Im Abschnitt "Ereignisse" können Sie auswählen, ob VirusBarrier X6 einen Scanvorgang automatisch ausführen, Reparaturen durchführen oder keine Aktion durchführen soll, wenn bestimmte Ereignisse eintreten.

Das erste Ereignis, **Wenn Laufwerke angemeldet sind:**, wird ausgelöst, wenn Sie ein neues Speichergerät auf dem Schreibtisch anmelden, entweder lokal (eine Festplatte) oder entfernt (ein Netzwerklaufwerk). Wenn das Kontrollkästchen **Außer schreibgeschützte Laufwerke** aktiviert ist, führt VirusBarrier X6 die Aktion nur auf den Datenträgern aus, auf denen das Programm das gescannte Laufwerk ändern kann (z. B., um eine infizierte Datei auf einem Datenträger zu reparieren).

Mit dem zweiten Ereignis, **Nach neuen Versionen der Virusdefinitionen:** können Sie VirusBarrier X6 anweisen, was nach dem Herunterladen von Programmen und der Installation neuer Virusdefinitionen und Filter ausgeführt werden soll. Virusdefinitionen und Filter werden regelmäßig aktualisiert. Und selbstverständlich dann, wenn eine neue schädliche Software entdeckt wurde, um vor dieser Gefahr zu schützen. Deshalb sollten Sie nach diesem Ereignis einen Scanvorgang durchführen, um nach dieser neuen schädlichen Software zu suchen. Dies können Sie manuell oder automatisch (durch Aktivieren dieses Kontrollkästchens) durchführen.

Im Abschnitt **Zeitpläne** können Sie festlegen, wann VirusBarrier X6 automatische Scanvorgänge ausführen soll.

Um das Planen zu aktivieren, klicken Sie auf das Kontrollkästchen "Zeitpläne aktivieren".

Unter diesen Einstellungen ist die Zeitplanauswahl. Hier können Sie festlegen, welcher Ordner wann überprüft werden soll.

- Im ersten Popup-menü können Sie auswählen, ob Sie die ausgewählten Dateien zum geplanten Zeitpunkt scannen, schnell scannen oder reparieren möchten. Wenn Sie "Schneller Scan" wählen, können Sie keine bestimmten Ordner auswählen, die gescannt werden sollen. Das zweite Menü wird ausgeblendet.
- Im zweiten Popup-Menü sind die Ordner aufgelistet, die Sie am wahrscheinlichsten scannen möchten, einschließlich Ihres Benutzerordners und Ihres Ordners "Dokumente". Die Standardauswahl ("Computer") weist VirusBarrier X6 an, alle Ordner von allen Benutzern auf Ihrem Mac zu scannen.
- Im dritten Popup-Menü können Sie auswählen, ob Sie den Vorgang jeden Tag, jede Woche oder jeden Monat durchführen möchten. Wenn Sie "Täglich" wählen, können Sie die von Ihnen bevorzugte Zeit auswählen. Wenn Sie "Wöchentlich" wählen, können Sie auch Ihren bevorzugten Tag auswählen. Wenn Sie "Monatlich" wählen, können Sie auswählen, an welchem Tag im Monat der Scanvorgang durchgeführt werden soll.

Es ist möglich, Zeitpläne mit mehreren Elementen zu erstellen. Wenn Sie beispielsweise Ihren Ordner "Dokumente" jeden Abend und Ihren gesamten Computer einmal pro Woche scannen möchten. Klicken Sie hierzu auf das Pluszeichen (+) rechts vom Zeitplanelement: daraufhin wird darunter ein anderes Zeitplanelement angezeigt. Ändern Sie dieses Zeitplanelement wie gewünscht. Sie können auf diese Weise so viele Zeitplanelemente wie erforderlich hinzufügen. Wenn Sie ein Planelement entfernen möchten, klicken Sie daneben auf das Minuszeichen (-).

Die Reihenfolge der Zeitplanelemente ist unbedeutend. Wenn Sie zwei Scanvorgänge für die gleiche Uhrzeit geplant haben, werden sie gleichzeitig ausgeführt.

Nach dem Einrichten der Zeitpläne wird die Anzahl der anstehenden Zeitplanelemente im Übersichtsfenster von VirusBarrier X6 im Bereich "Zeitpläne" angezeigt. Wenn Sie alle anstehenden Zeitpläne ausschalten möchten, wechseln Sie zum Bildschirm "Zeitpläne und Ereignisse" und deaktivieren das Kontrollkästchen "Zeitpläne aktivieren".

Deaktivieren und Aktivieren des Echtzeit-Scanners

Vielleicht möchten Sie den Echtzeit-Scanner von VirusBarrier X6 manchmal deaktivieren. Zum Beispiel, wenn Sie eine große Anzahl von Dateien von einem Datenträger auf einen anderen kopieren möchten und wissen, dass diese Dateien nicht mit schädlicher Software infiziert sind. Wenn Sie den Echtzeit-Scanner dann ausschalten, werden Ihre Dateien etwas schneller kopiert. Wählen Sie zum Deaktivieren des Echtzeit-Scanner das Intego-Menü aus Ihrer Menüleiste und wählen Sie dann "VirusBarrier X6 > Echtzeit-Scanner". Die Markierung wird dann aus diesem Menüelement entfernt. Wenn Sie den Echtzeit-Scanner wieder einschalten möchten, wählen Sie die gleiche Option aus dem Intego-Menü.

Warnmeldungen bei schädlicher Software

Ein Scanvorgang kann mit Intego VirusBarrier X6 zwar – wie zuvor beschrieben – auch manuell gestartet werden, das Programm ist jedoch am effektivsten, wenn es im Hintergrund läuft. Wenn VirusBarrier X6 eine infizierte oder beschädigte Datei erkennt, kann das Programm Sie auf unterschiedliche Weise warnen. Das hängt davon ab, wie Sie Dateien scannen und welche Einstellungen Sie im Fensterabschnitt für die Scaneinstellungen dafür gewählt haben, wie der Echtzeit-Scanner mit infizierten Dateien umgehen soll.

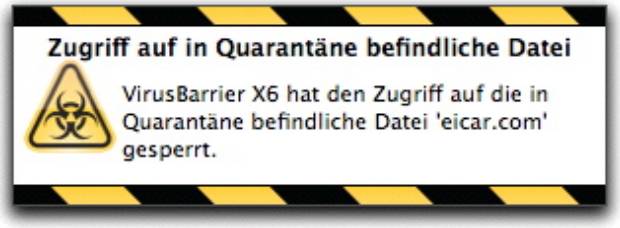
Wenn Sie bei aktiviertem Echtzeit-Scanner eine infizierte Datei aus dem Internet herunterladen oder sie von einer Festplatte oder einem anderen Speichermedium kopieren und wenn Sie den Scanner so eingestellt haben, dass er zuerst nachfragen soll, wenn infizierte Dateien entdeckt werden, dann wird VirusBarrier X6 die schädliche Software zuerst entdecken und dann einen Warnhinweis anzeigen.

VirusBarrier X6
Die Datei 'eicar.com' ist mit dem Virus 'Multi/Eicar' infiziert.
VirusBarrier X6 hat eine Gefahr auf Ihrem Computer entdeckt.
Im Finder anzeigen
Ignorieren
Unter Quarantäne stellen
Reparieren

Je nachdem, welche Art von Warnhinweis Sie gewählt haben und welche Optionen Sie eingestellt haben, erhalten Sie dann eine Anzahl von Auswahlmöglichkeiten. Wenn Sie auf "Im Finder anzeigen" klicken, wird die Datei auf Ihrer Festplatte angezeigt. Falls Sie möchten, dass VirusBarrier X6 die Datei repariert, klicken Sie auf "Reparieren". Soll die Datei in die Quarantänezone, klicken Sie auf "Unter Quarantäne stellen". (Weitere Informationen erhalten Sie im Abschnitt "Quarantäne" weiter hinten in diesem Kapitel). Wenn Sie keine Aktion durchführen möchten, klicken Sie auf die Schaltfläche "Ignorieren".

ACHTUNG: Das Ignorieren von Warnhinweisen kann gefährlich sein! Wählen Sie diese Option nur, wenn Sie auch wirklich wollen, dass infizierte Dateien nicht repariert werden.

Wenn Sie VirusBarrier X6 so eingestellt haben, dass infizierte Dateien in die Quarantänezone verschoben werden oder dass die Dateien repariert werden, wird ein kleiner Warnhinweis angezeigt.


Zugriff auf in Quarantäne befindliche Datei
VirusBarrier X6 hat den Zugriff auf die in Quarantäne befindliche Datei 'eicar.com' gesperrt.

Wenn Sie die Objekte scannen, indem Sie diese auf die Kugel von VirusBarrier X6 ziehen, wird der Warnhinweis in einem Dialogfeld vor dem Fenster von VirusBarrier X6 angezeigt.

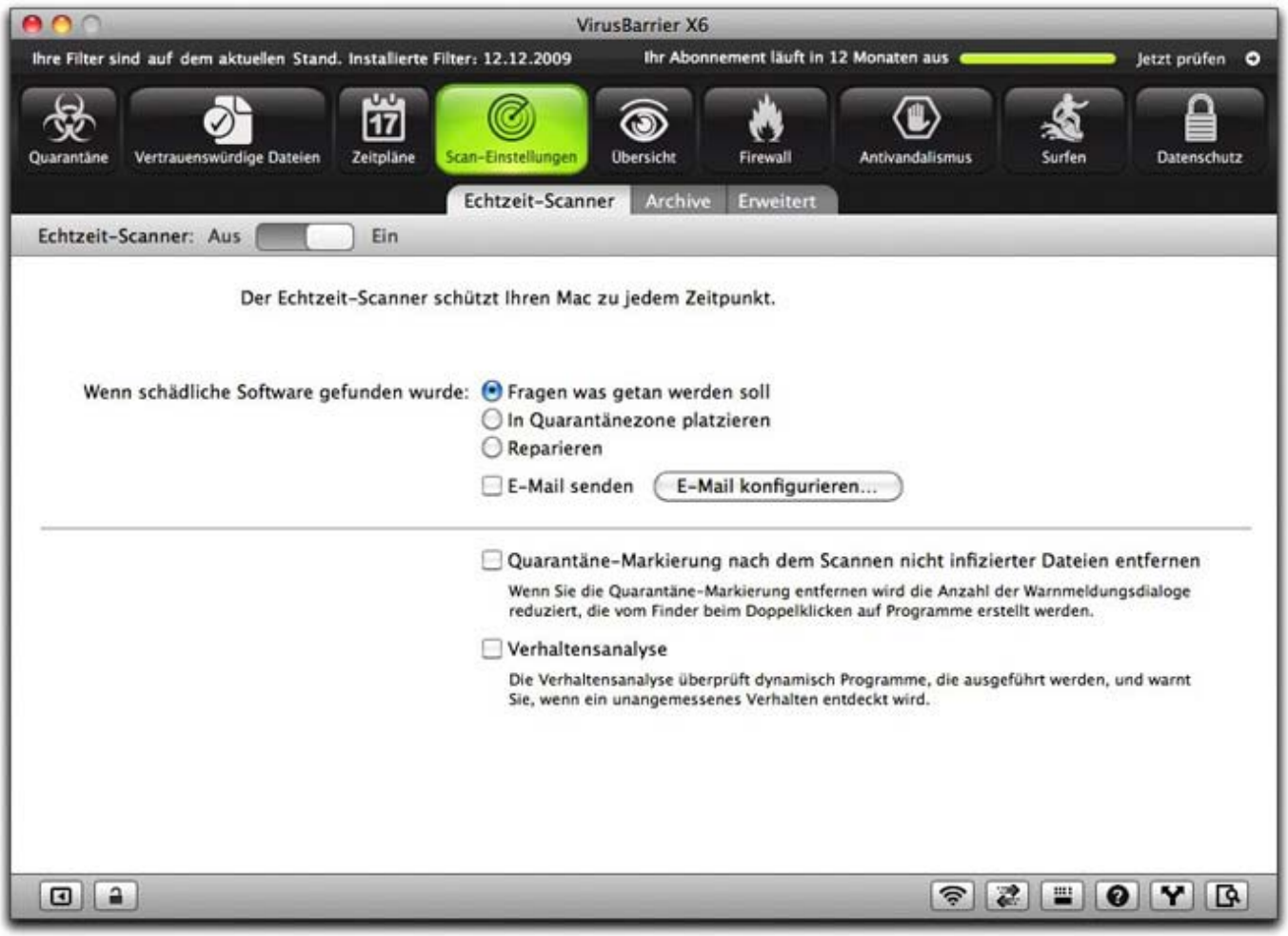
Wenn Sie innerhalb einer Minute nicht auf einen Warnhinweis des Echtzeit-Scanners reagieren, verschiebt VirusBarrier X6 die Datei in die Quarantänezone. (Das trifft nicht bei manuellen Scanvorgängen zu. Wenn Sie Dateien manuell scannen, wird der Warnhinweis solange angezeigt, bis Sie reagieren.) Sie können die Dateien später in der Quarantänezone überprüfen, um zu entscheiden, was sie damit tun möchten. Weitere Informationen finden Sie weiter hinten in diesem Kapitel im Abschnitt "Quarantäne".

Weitere Informationen über die Einstellungen der Warnhinweise finden Sie unter Einstellungen und Konfigurationen für VirusBarrier X6.

Scan-Einstellungen

VirusBarrier X6 bietet Ihnen verschiedenen Optionen, mit denen Sie das Programm anweisen können, wie Ihr Mac gescannt werden soll, welche Dateitypen gescannt werden sollen und nach welcher Art von schädlicher Software gesucht werden soll. Sie erhalten Zugriff auf diese Einstellungen, indem Sie auf die Schaltfläche "Scan-Einstellungen" klicken.

Der Fensterabschnitt für Scan-Einstellungen enthält drei Registerkarten: Echtzeit-Scanner - mit dieser Registerkarte wird gesteuert, wie VirusBarrier X6 Scanvorgänge im Hintergrund ausführt. Archive - mit dieser Registerkarte wird VirusBarrier X6 mitgeteilt, ob und welche Art von Archiven gescannt werden sollen. Erweitert - diese Registerkarte bietet weitere Einstellungen für den Echtzeit-Scanner und für den Scanner auf Abruf.



Einstellungen für den Echtzeit-Scanner

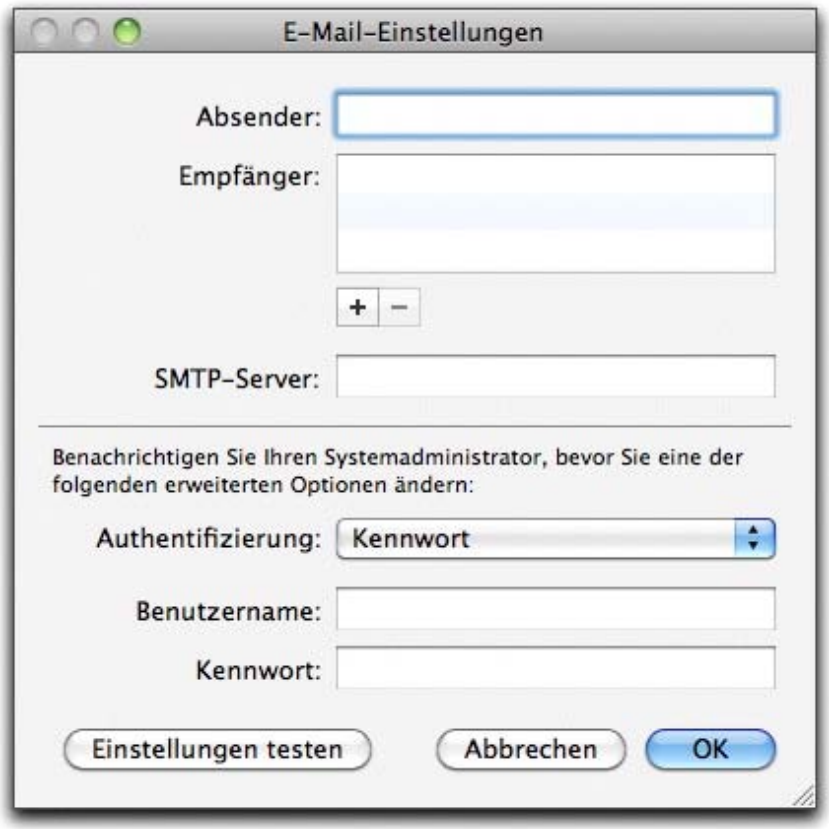
Wenn Sie den Echtzeit-Scanner ausschalten möchten, schieben Sie den Schieberegler für den Echtzeit-Scanner auf "Aus". Sie können ihn wieder einschalten, indem Sie den Schieberegler auf "Ein" schieben. Im normalen Betrieb brauchen Sie den Echtzeit-Scanner nicht deaktivieren. Das ist nur hilfreich bei der Fehlersuche, wenn Sie ein Problem mit Ihrem Mac haben. Sie können den Echtzeit-Scanner auch im Intego-Menü deaktivieren und aktivieren. Wählen Sie

hierzu "VirusBarrier X6 > Echtzeit-Scanner".

Mit der nächsten Einstellung können Sie festlegen, was VirusBarrier X6 machen soll, wenn schädliche Software gefunden wurde. Sie haben folgende Optionen:

- **Fragen was getan werden soll**: Diese Option ist am besten geeignet, wenn Sie beim Scanvorgang eines Macs anwesend sind, d. h., Sie verfolgen den Scanvorgang und sehen sofort, wenn ein Warnhinweis angezeigt wird. Beachten Sie, dass VirusBarrier X6 infizierte Dateien in die Quarantänezone verschiebt, wenn Sie innerhalb einer Minute nicht auf einen Warnhinweis reagieren.
- **In Quarantänezone platzieren**: Diese Option gewährleistet, dass die Datei nicht geöffnet oder gelesen werden kann. (Weitere Informationen zur Verwendung der Quarantänezone finden Sie weiter hinten im Abschnitt "Quarantänezone".)
- **Reparieren**: Diese Option weist VirusBarrier X6 an, zu versuchen, die schädliche Software zu entfernen. Wenn die Datei aus irgendeinem Grund nicht repariert werden kann, wird sie in die Quarantänezone verschoben.

Außerdem können Sie festlegen, dass VirusBarrier X6 Ihnen bei einem Virusfund eine E-Mail senden soll. Wenn Sie dies einrichten möchten, aktivieren Sie das Kontrollkästchen **E-Mail senden**, und klicken Sie dann neben dem Kontrollkästchen auf die Schaltfläche **E-Mail konfigurieren…**. Daraufhin wird das Fenster mit den Mail-Einstellungen angezeigt.



Sie müssen die E-Mail-Adressen für den Absender und den oder die Empfänger und den Namen des SMTP-Servers (für ausgehende E-Mail-Nachrichten) eingeben. Zudem müssen Sie einen Benutzernamen und ein Passwort eingeben, die Ihr Mailserver akzeptiert. E-Mails können an mehrere Empfänger versendet werden. Klicken Sie auf das Pluszeichen (+), um einen Empfänger hinzuzufügen. Klicken Sie auf das Minuszeichen (-), um einen Empfänger zu löschen.

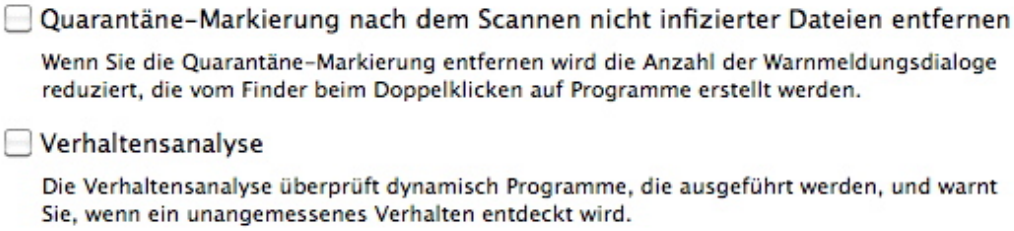
Die untere Hälfte des Fensters für die E-Mail-Einstellungen enthält erweiterte Optionen, die VirusBarrier X6 eventuell für den E-Mail-Versand benötigt.

Das folgende Dropdown-Menü zeigt verschiedene Arten der verwendeten E-Mail-Authentifizierungen.

Sie sollten die gleiche Authentifizierung sowie den gleichen Benutzernamen und das gleiche Passwort verwenden, die Sie in Ihrem Standard-E-Mail-Programm benutzen. Wenn Sie nicht sicher sind, was Sie hier eingeben sollen, fragen Sie Ihren ISP oder Ihren Systemadministrator. Wenn Sie nicht wissen, welche Art der Authentifizierung Sie verwenden, wählen Sie die Option "Automatisch".

Wenn Sie fertig sind, können Sie bestätigen, dass die E-Mail-Nachricht beim Empfänger ankommt, indem Sie auf die Schaltfläche "Einstellungen testen" klicken. Sie müssen eventuell mehrere Sekunden warten, bevor Ihr Mailserver reagiert. Nach dem Test werden in einem Dialogfeld die Testergebnisse angezeigt.

Im nächsten Abschnitt des Fensters für die Einstellungen des Echtzeit-Scanners können Sie zwei Einstellungen aktivieren.

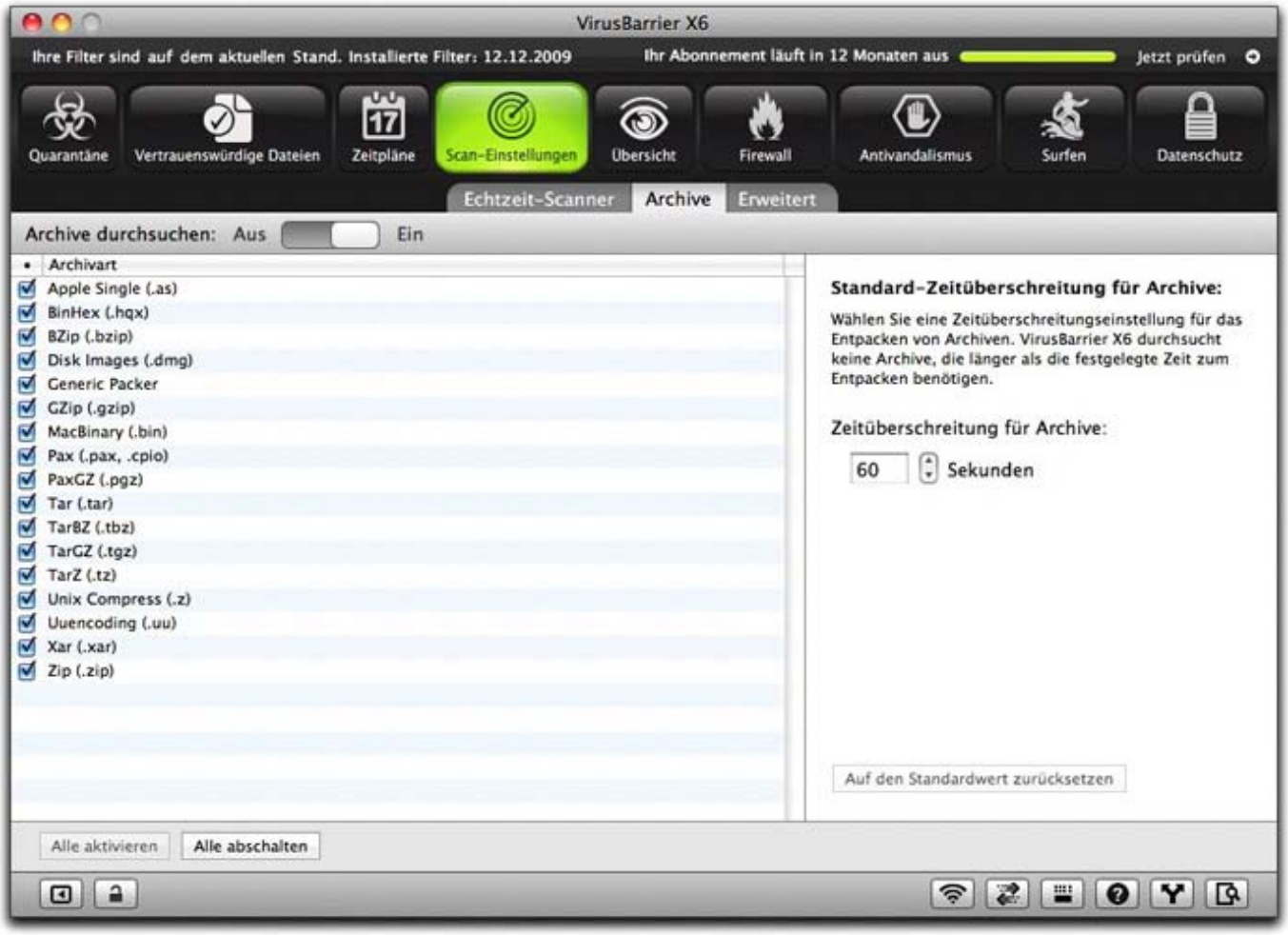

Quarantäne-Markierung nach dem Scannen nicht infizierter Dateien entfernen
Wenn Sie die Quarantäne-Markierung entfernen wird die Anzahl der Warnmeldungsdialoge reduziert, die vom Finder beim Doppelklicken auf Programme erstellt werden.
Verhaltensanalyse
Die Verhaltensanalyse überprüft dynamisch Programme, die ausgeführt werden, und warnt Sie, wenn ein unangemessenes Verhalten entdeckt wird.

Die erste Option, **Quarantäne-Markierung nach dem Scannen nicht infizierter Dateien entfernen** weist VirusBarrier X6 an, die Quarantäne-Markierung zu entfernen, die Mac OS X setzt, wenn Programme heruntergeladen werden und VirusBarrier X6 festgestellt hat, dass diese nicht durch irgendeine schädliche Software infiziert sind. So wird das Mac OS X-Dialogfeld entfernt, in dem Sie vor den heruntergeladenen Dateien gewarnt und gefragt werden, ob Sie diese wirklich öffnen möchten.

Die zweite Option, **Verhaltensanalyse**, weist VirusBarrier X6 an, die Verhaltensanalyse zu verwenden, um von Programmen ausgeführte verdächtige Aktivitäten im Auge zu behalten. Wenn irgendein Programm irgendetwas macht, das als nicht normal betrachtet werden kann (wie zum Beispiel eine große Anzahl von Dateien löschen), warnt VirusBarrier X6 Sie davor.

Archiv-Einstellungen

Archive enthalten eine oder mehrere Dateien, die gewöhnlich komprimiert sind, damit sie einfach und schnell übertragen werden können. VirusBarrier X6 guckt in viele bekannte Archivtypen hinein und scannt dabei nicht nur die Archiv-Datei selbst, sondern auch die Dateien, die das Archiv enthält.

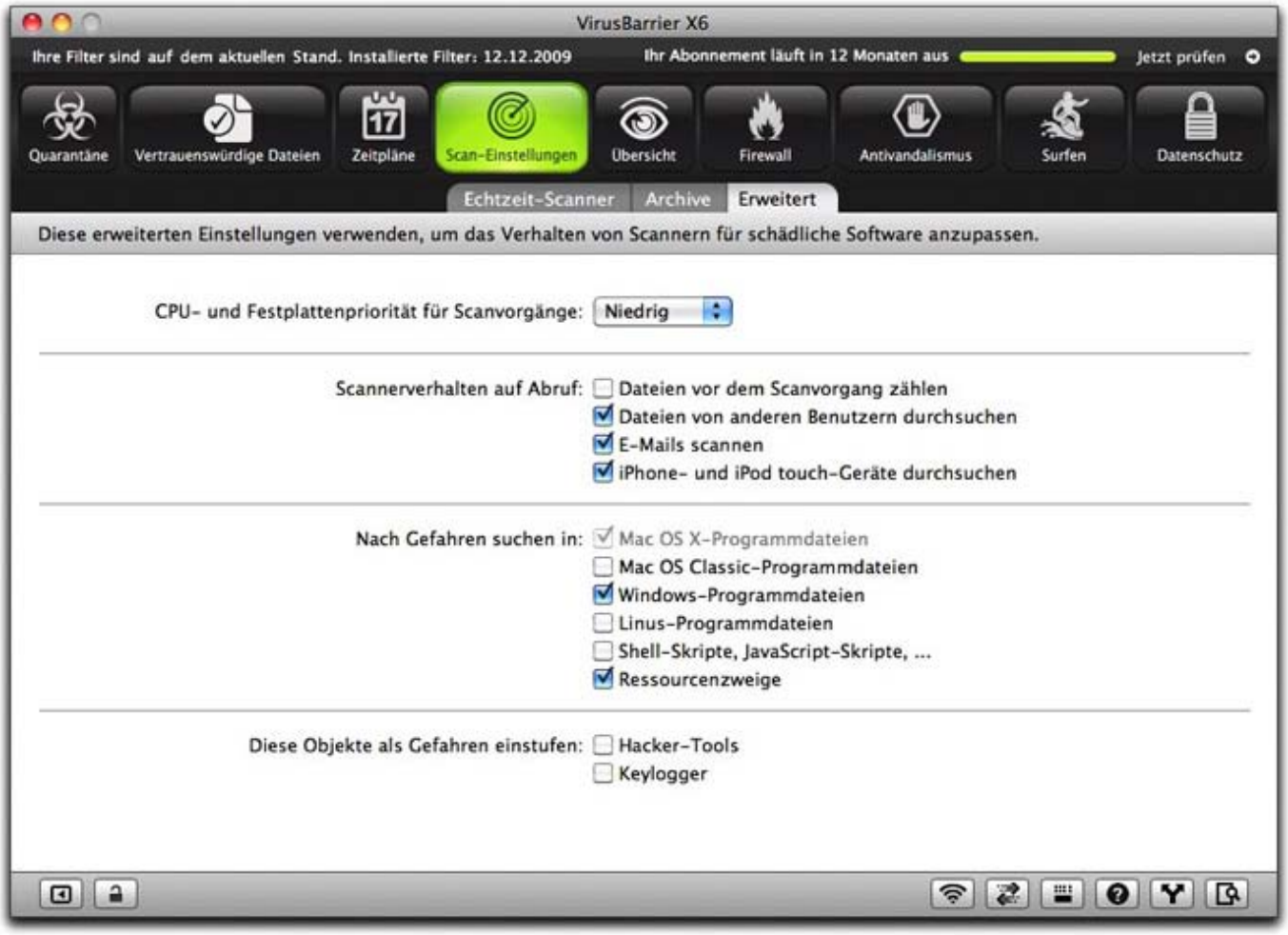


Standardmäßig scannt VirusBarrier X6 alle Archivtypen, die das Programm versteht. Sie können jedoch auswählen, dass nur bestimmte Archivtypen gescannt werden sollen, indem Sie die Markierung der verschiedenen Archivtypen in der Liste mit den Archivarten entfernen. Wenn Sie manuelle Scanvorgänge ausführen, können Sie auch alle Archive, während sie überprüft werden, überspringen, indem Sie auf die Schaltfläche "Überspringen" in der Kugel von VirusBarrier X6 klicken. Das ist eventuell bei großen Archiven sinnvoll, bei denen die Analyse sehr lange dauert – sofern Sie sicher sind, dass diese frei von schädlicher Software sind.

Mit der Standardeinstellung für die Zeitüberschreitung bei Archiven können Sie VirusBarrier X6 anweisen, das Scannen von Archiven zu stoppen, wenn es länger als eine bestimmte Zeit dauert, sie zu entpacken und zu scannen. Standardmäßig sind "60 Sekunden" eingestellt. Alle Dateien, die vor dieser Zeitüberschreitung entpackt wurden, werden jedoch gescannt.

Erweiterte Scan-Einstellungen

Die Registerkarte "Erweitert" bietet eine Reihe von Einstellungen für den Scanner auf Abruf sowie einige allgemeine Scan-Einstellungen.



Die erste verfügbare Option ist die CPU- und Festplatten-Priorität für Scanvorgänge. Sie können aus einem Popup-Menü zwischen "Niedrig" "Normal" oder "Hoch" wählen. Diese Einstellungen gelten für manuelle Scanvorgänge und geplante Scanvorgänge und weisen VirusBarrier X6 an, das Scannen so anzupassen, dass andere Programme dadurch nicht langsamer werden. Diese Einstellung wirkt sich sowohl auf den Prozessor (CPU) für den Scanvorgang als auch auf das Lesen Ihrer Festplatte(n) aus. Beachten Sie, dass sich diese Einstellung auch auf Scanvorgänge auswirkt, die automatisch ausgeführt werden, wenn Sie einen externen Datenträger auf dem Schreibtisch anmelden oder nachdem Sie die Filter für VirusBarrier X6 aktualisiert haben. Wenn Sie also möchten, dass diese Scanvorgänge schneller abgeschlossen werden, sollten Sie "Normal" oder "Hoch" wählen. Wenn es Ihnen egal ist, wie lange diese Scanvorgänge dauern oder wenn Sie möchten, dass Ihr Mac die höhere Priorität hat, dann wählen Sie "Niedrig".

Vier Optionen beeinflussen das Verhalten des Scanners auf Abruf:

- Mit der Option **Dateien vor dem Scanvorgang zählen** weisen Sie VirusBarrier X6 an, die zu scannenden Dateien zu zählen. Hierdurch erhalten Sie genauere Informationen über die Dauer des Scanvorgangs. Während eines manuellen Scanvorgangs werden die Anzahl der Dateien und der Prozentsatz der gescannten Dateien in der Kugel angezeigt. Wenn diese Option markiert ist, zählt die Kugel von VirusBarrier X6 während des Scanvorgangs rückwärts und zeigt an, wie viele Dateien noch überprüft werden müssen. Wenn sie nicht markiert ist, zählt die Kugel während des Scanvorgangs vorwärts und zeigt an, wie viele Dateien bereits gescannt wurden.
- Mit der Option **Dateien von anderen Benutzern durchsuchen** erlauben Sie, dass VirusBarrier X6 nicht nur die Dateien nach schädlicher Software durchsucht, die zu dem Benutzerkonto gehören, das beim Start des Scanvorgangs angemeldet ist. Es werden auch Dateien eingeschlossen, die anderen Benutzern gehören. Wenn Sie diese Option auswählen, müssen Sie sofort ein Administratorpasswort eingeben. Wenn Sie dieses Passwort nicht kennen, wird das Kontrollkästchen wieder deaktiviert. Wenn Sie diese Option nicht auswählen und VirusBarrier X6 eine mit einem Virus infizierte Datei findet, die einem anderen Benutzer oder dem System

gehört, wird im Warnhinweis- und Quarantänezonefenster von VirusBarrier X6 ein durchgestrichener Stift angezeigt. Dieses Symbol weist darauf hin, dass Sie den Benutzernamen und das Kennwort eines Administrators eingeben müssen, um eine Aktion an dieser Datei auszuführen.
- **E-Mails scannen.** VirusBarrier X6 scannt während eines manuellen Scanvorgangs den Inhalt und alle Anhänge von ein- und ausgehenden E-Mails.
- **iPhone/iPod touch scannen** weist VirusBarrier X6 an, alle iPhones oder iPod touch-Geräte anzuzeigen, die mit Ihrem Mac verbunden sind, wenn Sie einen manuellen Scanvorgang ausführen. So können Sie auswählen, ob auch dieses Gerät nach schädlicher Software durchsucht werden soll. Wenn diese Option nicht aktiviert ist, zeigt VirusBarrier X6 kein iPhone oder keinen iPod touch in seinem Browser an.

Im Bereich **Nach Gefahren suchen in:** können Sie auswählen, ob VirusBarrier X6 bestimmte Dateien oder Programme scannen soll:

- **Schädliche Software für Mac OS X**: Diese Option ist abgeblendet, da sie immer aktiv ist. VirusBarrier X6 sucht immer nach schädlicher Software für Mac OS X. Dazu zählen alle Arten von schädlicher Software, die Mac OS X betrifft (z. B. Word- und Excel-Makroviren). Die anderen Kategorien sind Arten schädlicher Software, die Mac OS X nicht beschädigen können.
- **Schädliche Software für Mac OS Classic**: Schädliche Software, die nur Mac OS Classic betrifft. Wenn Sie noch Programme für Mac OS Classic verwenden, können Sie diese Optionen markieren. Wenn nicht, lassen Sie diese Option unmarkiert.
- **Schädliche Software für Windows**: Wenn Sie diese Option markieren, sucht VirusBarrier X6 nach Viren, die Windows betreffen. Obwohl diese Dateien Ihren Mac nicht beschädigen können, könnten Sie sie an Freunde weiterleiten, die Windows verwenden. Diese Dateien könnten Sie betreffen, wenn Sie Windows auf Ihrem Apple Computer mittels eines Programms wie Apple Boot Camp, VMware Fusion oder Parallels Desktop verwenden. (VirusBarrier X6 scannt jedoch keine virtuellen Windows-Festplatten).
- **Schädliche Software für Linux**: Wenn diese Option markiert ist, sucht VirusBarrier X6 nach schädlicher Software, die das Betriebssystem Linux betrifft.
- **Schädliche Skripte**: Wenn Sie diese Option markieren, sucht VirusBarrier X6 nach schädlichen Skripten, wie z.B. PHP, Shell-Skripten, Java-Skripten, Perl, etc.
- **Beschädigte Ressourcenzweige**: Bei dieser Art von beschädigter Datei handelt es sich zwar nicht notwendigerweise um schädliche Software, beschädigte Ressourcenzweige (Teile von bestimmten Dateien) können aber in bestimmten Fällen zum Absturz von Macs führen. Wenn Sie diese Option markieren, können Sie Ihren Mac vor Abstürzen durch dieses Art von beschädigten Dateien schützen.

Im letzten Abschnitt können Sie auswählen, ob nach zwei anderen Arten schädlicher Software gesucht werden soll:

- **Hacker-Tools** sind schädliche Programme, die Ihren Mac vielleicht nicht direkt schädigen, die aber von Hackern verwendet werden können, um andere Computer anzugreifen. Es ist besonders hilfreich diese Option zu markieren, wenn Ihr Mac öffentlich zugänglich ist.
- **Keylogger** sind Programme, die alle Ihre Tasteneingaben aufzeichnen. Bei einigen dieser Programme handelt es sich um schädliche Software, andere wurden aber eventuell auch absichtlich installiert, um Computerbenutzer (z.B. Kinder) zu überwachen. Wenn diese Option markiert ist, werden überwachte Benutzer möglicherweise gewarnt, dass diese Art von Software auf ihrem Mac vorhanden ist.

Vertrauenswürdige Dateien

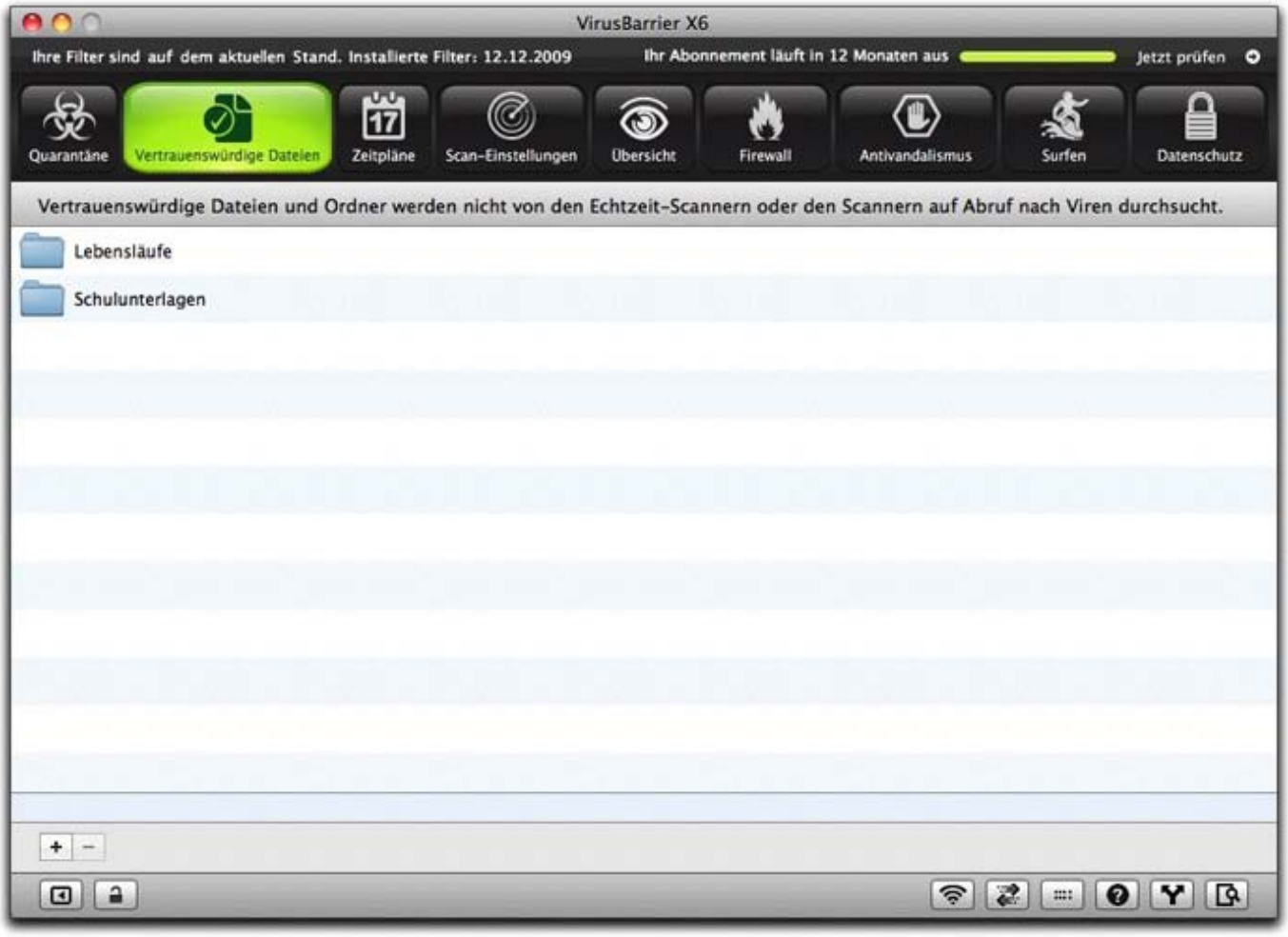
In VirusBarrier X6 können Sie Dateien, Ordner oder Datenträger einer Liste mit vertrauenswürdigen Dateien hinzufügen. VirusBarrier X6 geht dann davon aus, dass diese Dateien sicher sind und durchsucht sie nicht nach schädlicher Software. Sie sollten diese Option ausschließlich für sichere Dateien verwenden, die bereits mit VirusBarrier X6 gescannt wurden.

Sie können Dateien, Ordner und Laufwerke auf zwei verschiedene Arten der Liste mit vertrauenswürdigen Dateien hinzufügen. Klicken Sie zuerst auf die Schaltfläche "Vertrauenswürdige Dateien".

Führen Sie dann einen der folgenden Schritte aus:

- Klicken Sie auf das kleine Pluszeichen (+) in der unteren linken Ecke des Fensters, navigieren Sie zu dem Objekt, das Sie der Liste mit vertrauenswürdigen Dateien hinzufügen möchten und klicken Sie dann auf die Schaltfläche "Hinzufügen". Oder
- ziehen Sie das Objekt aus dem Finder in das Fenster.

Wenn Sie einen Ordner oder ein Laufwerk hinzufügen, geht VirusBarrier X6 davon aus, dass *alle* Dateien, die im ausgewählten Objekt und den darin enthaltenen Unterordnern enthalten sind, vertrauenswürdig sind.



Wenn Sie ein Objekt von der Liste mit vertrauenswürdigen Dateien entfernen möchten, müssen Sie es nur auswählen und dann auf die Schaltfläche "-" klicken.

Sie können auch das Kontextmenü verwenden, um der Liste mit vertrauenswürdigen Dateien Objekte hinzuzufügen: Im Abschnitt über das Kontextmenü weiter hinten in diesem Kapitel erhalten Sie weitere Informationen.

Quarantänezone

Wenn Sie Dateien nicht automatisch reparieren lassen möchten, kann VirusBarrier X6 diese Dateien in seiner Quarantänezone ablegen. Dateien in der Quarantänezone können weder geöffnet noch gelesen werden. Auf diese Weise wird gewährleistet, dass die Dateien Ihren Mac nicht infizieren können. Dies ist nützlich für Administratoren, die die Dateien überprüfen möchten, bevor sie die Reparaturfunktionen von VirusBarrier X6 ausführen.

Wie bereits weiter oben bei der Erklärung von Warnhinweisen erwähnt, verschiebt VirusBarrier X6 Dateien automatisch in die Quarantänezone, wenn Sie innerhalb einer Minute nicht auf einen Warnhinweis reagieren. Sie können diese Dateien dann überprüfen und entscheiden, was getan werden soll. Die Schaltfläche "Quarantäne" im Übersichtsfenster von VirusBarrier X6 zeigt Ihnen an, welche Dateien sich in Quarantäne befinden.

Wenn Sie sehen möchten, welche Dateien sich in Quarantäne befinden, klicken Sie entweder auf diese Schaltfläche oder klicken Sie auf die Schaltfläche "Quarantäne" am oberen Fensterrand.

In einer Anzeige sehen Sie die Dateien, die in der Quarantänezone sind. Außerdem werden mehrere Schaltflächen angezeigt, mit denen Sie Aktionen für diese Dateien durchführen können.

Sie können sich Dateien in Quarantäne als Symbole oder als Listenobjekte anzeigen lassen, indem Sie auf eine der Ansichtsschaltflächen oben links im Fenster klicken.

Wenn Sie eine Aktion für eine der Dateien durchführen möchten, wählen Sie diese aus und klicken Sie unten rechts im Fenster auf eine der vier Schaltflächen.

Sie können folgende Aktionen durchführen:

- **Vom Datenträger löschen** entfernt die Datei von Ihrem Mac.
- Wenn Sie **Als sicher einstufen** wählen, geht VirusBarrier X6 davon aus, dass Sie diese Datei für nicht infiziert halten und fügt diese Datei der Liste mit vertrauenswürdigen Dateien von VirusBarrier X6 hinzu. Dies kann bei Dateien vorkommen, die fälschlicherweise als infiziert eingestuft wurden. Seien Sie jedoch *sehr vorsichtig*, wenn Sie auf diese Schaltfläche klicken. Tun Sie es nur, wenn Sie wirklich wissen, dass diese Datei sicher ist. Andernfalls infiziert die Datei eventuell den gesamten Mac.
- Wenn Sie **Scannen** wählen, scannt VirusBarrier X6 Datei noch einmal. Das sollten Sie eventuell nach der Aktualisierung der Virusdefinitionen machen, damit Sie sicher gehen, dass diese Datei nicht fälschlicherweise als "False-Positive" markiert wurde.
- Wenn Sie **Reparieren** wählen, entfernt VirusBarrier X6 die schädliche Software aus der Datei.

Wenn Sie sich die Quarantänezone im Listenmodus anzeigen lassen, wird in der Spalte "Gefahr" angezeigt, mit welcher Art von schädlicher Software Ihre Dateien infiziert sind.

Das Kontextmenü für VirusBarrier X6

Mit dem Kontextmenü haben Sie direkt aus dem Finder Zugriff auf viele Funktionen von VirusBarrier X6. Halten Sie hierzu einfach die Steuerungstaste gedrückt und klicken Sie auf ein beliebiges Objekt (eine Datei, einen Ordner oder einen Datenträger) oder klicken Sie mit der rechten Maustaste auf ein beliebiges Objekt. Dann wird ein Kontextmenü geöffnet. Unter Mac OS X 10.6 (Snow Leopard) sind diese Menüelemente am unteren Rand des Kontextmenüs gruppiert. Wenn es jedoch genügend solcher Elemente gibt, wird Ihnen das Menüelement "Dienste" angezeigt und die Menüelemente von VirusBarrier X6 befinden sich im Untermenü von "Dienste". Unter Mac OS X 10.5 (Leopard) wird das Menü von VirusBarrier X6 unter dem Menü "Mehr" angezeigt.

Das Kontextmenü bietet Ihnen folgende Möglichkeiten:

- Das ausgewählte Objekt scannen (und reparieren, sofern Ihre Einstellungen dies zulassen).
- Senden Sie eine Kopie des Objekts an Intego, indem Sie "Verdächtige Datei an Intego senden" auswählen. Dies ist besonders nützlich, wenn Sie Dateien haben, bei denen Sie vermuten, dass sie mit neuen oder nicht erkannten Viren infiziert sind. Wenn Sie diese Option wählen, können die Virusexperten von Intego die Datei überprüfen und wenn nötig die Virusdefinitionen erstellen, die Sie und andere Benutzer zum Schutz Ihrer Systeme benötigen.
- Das Objekt der Liste mit vertrauenswürdigen Dateien hinzufügen.

Verwenden von VirusBarrier X6 über die Befehlszeile

VirusBarrier X6 gibt Ihnen auch die Möglichkeit, Suchvorgänge nach schädlicher Software und Änderungen an den Einstellungen für den Netzwerkschutz über die Befehlszeile durchzuführen. Im Folgenden wird die Verwendung dieses Befehls beschrieben.

```
Befehl:
/Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers
Die folgenden Optionen sind verfügbar:
```

```
        -a:    Scannt alle Dateien, einschließlich derer, die mit einer symbolischen Verknüpfung mit
anderen
               Datenträgern (oder anderen Mount-Punkten in /Volumes) verbunden sind.
        -c:    Zählt Dateien vor dem Scanvorgang.
        -C:    Zählt Dateien, es wird jedoch kein Scanvorgang durchgeführt.
        -Q:    Führt einen schnellen Scanvorgang aus.
        -r:    Repariert infizierte Dateien.
        -t:    Verwendet den Turbomodus; scannt nur die Dateien, die seit dem letzten Scanvorgang
               nicht geändert wurden.
        -T:    Scannt alle Dateien außer den vertrauenswürdigen.
        -z:    Scannt komprimierte Archive (einschließlich derer in E-Mail-Anhängen).

        <zu_scannender_Pfadname>: Erforderlich; dies kann ein relativer oder absoluter Pfad sein.

        [<Pfadname_aktuelles_Verzeichnis>]: Das ist optional. Es ist das aktuell funktionierende
        Verzeichnis, wenn ein relativer Pfad als erstes Argument verwendet wird.

        Beispiel:

        /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers -tacz /

        Scannt alle Laufwerke, für die der Benutzer eine Leseerlaubnis hat, scannt Archive
        und zählt vor dem Start die Anzahl der Dateien, die gescannt werden sollen. Wenn Sie den
        Befehl mit dem vorangestellten Argument "sudo" ausführen und eine Authentifizierung durchführen,
        können Sie alle Dateien scannen.

        Sie können auch Aliasse definieren, um die Verwendung dieses Befehls zu vereinfachen.

        Für bash:

        alias vbscan=/Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers

        Für tcsh:

        alias vbscan /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers

        So können Sie den gleichen Befehl wie folgt ausführen:

        vbscan -tacz / [-rtcCaz] <zu_scannender_Pfadname> [<Pfadname_aktuelles_Verzeichnis>]

        Wenn Sie die Einstellungen für den Netzwerkschutz ändern möchten, verwenden Sie die folgende
Option
        zusammen mit den Vorgängen, Objekten und Daten, die unten aufgeführt sind (alle Befehle mit
        Firewall-Optionen erfordern "sudo"):

        -W: Firewallvorgänge ausführen

        Vorgang             Objekt                                Daten
        ------------------------------------------------------------------
        import|export       settings                              file_path
        revert              settings
        add|remove          blocked_address|trusted_address       ip_address
        print               blocked_address|trusted_address
        get                 protection
        enable/disable      protection
        enable/disable      trojans
        enable/disable      data
        enable/disable      antispyware
        enable/disable      banner_filter
        enable/disable      cookie_filter
        enable/disable      information_filter
        enable/disable      webthreats
        enable/disable      antiphishing
        activate            configuration                         configuration_name
        print               configuration
        reset               traffic
        reset               cookie

        Um beispielsweise den Firewallschutz zu aktivieren, führen Sie den folgenden Befehl mit "sudo"
aus:

        /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers -W enable protection
```

Verwenden von VirusBarrier X6 und AppleScript

VirusBarrier X6 bietet die Möglichkeit, Scanvorgänge mit AppleScript auszuführen. Weitere Informationen über die AppleScript-Syntax des Programms erhalten Sie im VirusBarrier X6-Wörterbuch von Script Editor.

© 2009 Intego. Alle Rechte vorbehalten.

So schützen Sie Ihren Mac vor Netzwerkangriffen

- So verwenden Sie das Übersichtsfenster von VirusBarrier X6
- Statusanzeigen im Übersichtsfenster
- Firewall-Schutz
- Schutz vor Trojanischen Pferden
- Antivandalismus-Schutz
- Gesperrte Adressen und Vertrauenswürdige Adressen
- Surffilter
- Schutz persönlicher Daten
- Die Bedeutung von Warnmeldungen

Zum Hauptinhaltsverzeichnis wechseln

Zusätzlich zu den leistungsstarken Funktionen zum Schutz vor schädlicher Software schützt VirusBarrier X6 Ihren Mac mit einer Vielzahl leistungsstarker Funktionen vor Netzwerkangriffen und Web Threats. Diese Funktionen können in vier Gruppen aufgeteilt werden:

- **Firewall**: Legt fest, welche Netzwerkkommunikation Ihr Mac zulässt.
- **Antivandalismus**-Tools: Überwachen die Kommunikation für sechs Arten vorsätzlicher Angriffe.
- **Surf**-Tools: Suchen nach Angriffen durch "soziale Manipulation", die auf Ihrem Online-Verhalten basieren, und schützt vor Web Threats.
- **Datenschutz**-Funktionen: Lassen Sie entscheiden, welche Programme sich mit einem Netzwerk verbinden und welche Daten sie nicht versenden dürfen.

Zusammen schützen diese vier Verteidigungsfunktionen Sie vor nahezu jeder Art von möglichen Angriffen - auch vor Trojanischen Pferden, Ping-Angriffen und Port-Scanning. In Verbindung mit dem Schutz vor schädlicher Software bietet VirusBarrier X6 einen vollständigen Schutz vor schädlicher Software und einen vollständigen Netzwerkschutz für Ihren Mac.

Wenn Sie VirusBarrier X6 starten, wird das Übersichtsfenster angezeigt. Sie können immer wieder zu diesem Fenster zurückkehren, indem Sie auf die Schaltfläche "Übersicht" in der Mitte der oberen Schaltflächenzeile klicken. Das Fenster ist in Spalten aufgeteilt: Links der mittleren Kugel befinden sich die Funktionen für den Schutz vor schädlicher Software, rechts befinden sich die Funktionen für den Netzwerkschutz, die wir Ihnen in diesem Kapitel erklären. Der Schutz vor schädlicher Software wird unter So schützen Sie Ihren Mac vor Viren und schädlicher Software erklärt.

So verwenden Sie das Übersichtsfenster von VirusBarrier X6

Über das Übersichtsfenster erhalten Sie einen schnellen Zugriff auf:

- Virenschutz-Tools, die unter So schützen Sie Ihren Mac vor Viren und schädlicher Software erklärt werden,
- Die Funktionen, Einstellungen und Protokolle von VirusBarrier X6,
- mehrere hilfreiche Netzwerkdienstprogramme, wie Whois und Traceroute,
- grafische Anzeigen dafür, welche Schutzarten aktiviert sind,
- Informationen über das Programm selbst, z.B. wann es zuletzt aktualisiert wurde,
- eine Möglichkeit mehrere Konfigurationen zu verwalten, damit Sie die Schutzeinstellungen schnell ändern können.

In der Mitte des Übersichtsfensters gibt es Bereiche, mit denen Sie die vier Verteidigungslinien von VirusBarrier X6 steuern können. Die Bedienelemente für Firewall-, Antivandalismus-, Surf- und Datenschutz sind die großen Schaltflächen oben rechts im Übersichtsfenster. Wenn sie ausgewählt werden, sind sie grün und wenn nicht, sind sie schwarz. Die kleineren Schaltflächen in der unteren rechten Ecke sind die Bedienelemente für die Überwachung. Zwischen diesen beiden Gruppen gibt es hilfreiche Anzeigen, die Sie zu den entsprechenden Bedienelementen führen, wenn Sie darauf klicken.

	Im Abschnitt "Firewall" erhalten Sie Zugriff auf die Regeln, die festlegen, welche Programme Informationen von Ihrem Mac versenden und darauf empfangen dürfen.

	Im Abschnitt "Antivandalismus" haben Sie verschiedene Möglichkeiten, bestimmte Arten von Netzwerkangriffen zu stoppen. Zudem können Sie Richtlinien auswählen, die festlegen, wie mit Angriffen umgegangen werden soll, wenn sie auftreten.
	Im Abschnitt "Surfen" werden das Versenden und Empfangen bestimmter Arten von Informationen gesperrt, während Sie im Internet surfen. So werden Sie vor Phishing-Versuchen, Werbung und Cookies geschützt. Mit dieser Funktion können Sie bestimmte Informationen verbergen, die Ihr Browser normalerweise übermittelt.
	Im Abschnitt "Datenschutz" haben Sie Zugriff auf Einstellungen, die verhindern, dass bestimmte Daten über das Internet oder lokale Netzwerke versendet werden. Die Anti-Spyware-Tools schützen Sie vor Programmen, die sich heimlich mit entfernten Computern verbinden.

Über die Schaltflächen in der unteren rechten Ecke des Übersichtsfensters können Sie auf die Überwachungsfunktionen zugreifen. Unter So verwenden Sie die Überwachungstools von VirusBarrier X6 erhalten Sie weitere Informationen über die Verwendung dieser Funktionen.

Sie können in VirusBarrier X6 verschiedenen Konfigurationen erstellen. Dabei handelt es sich um eine Gruppe von Einstellungen für die verschiedenen Funktionen des Programms. Eine Liste der Konfigurationen wird Ihnen angezeigt, wenn Sie auf die kleine Pfeil-Schaltfläche in der unteren linken Ecke des Übersichtsfensters klicken. (Sie können auch zwischen dem Ein- und Ausblenden der Konfigurationsliste hin- und herwechseln, indem Sie Befehlstaste-K drücken oder "Ansicht > Konfigurationen ein-/ausblenden" wählen.)

Zuerst gibt es nur eine Konfiguration, die entsprechend der von Ihnen vorgenommenen Einstellungen im Konfigurationsassistenten benannt ist, als Sie das Programm zum ersten Mal gestartet haben. Wenn Sie den Konfigurationsassistenten nicht ausgeführt haben, heißt sie "Standard". Das runde Optionsfeld zeigt an, welche Konfiguration gerade aktiv ist.

Am unteren Rand der Konfigurationsliste befindet sich eine Aktionsschaltfläche, mit der Sie die Konfigurationen duplizieren, bearbeiten und entfernen können. Weitere Informationen finden Sie unter Einstellungen und Konfigurationen für VirusBarrier X6.

Ganz oben im Übersichtsfenster befindet sich die NetUpdate-Statusleiste. Sie zeigt die Daten der neuesten VirusBarrier-Filter an, die auf Ihrem Mac installiert sind, sowie die Daten der neuesten Filter, die erhältlich sind. VirusBarrier X6 verwendet Intego NetUpdate, das mit dem Programm installiert wird, um Filter und Virusdefinitionen sowie die Intego-Programme selbst zu aktualisieren. NetUpdate sucht automatisch nach Aktualisierungen. Sie können das Programm auch sofort nach Aktualisierungen suchen lassen, indem Sie auf die Schaltfläche "Jetzt prüfen..." in der oberen rechten Ecke klicken. Wenn Sie die Statusleiste von NetUpdate ausblenden möchten, wählen Sie "Ansicht >

Statusleiste für NetUpdate ausblenden". Weitere Informationen über die Verwendung von NetUpdate finden Sie im Benutzerhandbuch von Intego für die ersten Schritte.

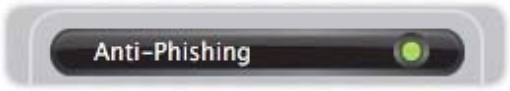
Statusanzeigen im Übersichtsfenster

Der Status verschiedener Netzwerkschutzfunktionen von VirusBarrier X6 wird als Stapel von Anzeigen in der rechten Spalte des Übersichtsfensters angezeigt, die Sie anklicken können.

Die oberste Anzeige informiert Sie darüber, welchen Firewall-Modus Sie ausgewählt haben. Wenn Sie darauf klicken, wird ein Fenster geöffnet, in dem Sie diese Einstellung ändern können. (Über die große Schaltfläche mit der Bezeichnung "Firewall" im oberen Fensterbereich gelangen Sie ebenfalls zu diesem Fenster.)

Netzwerk-Schutz
Firewall-Modus
Client, lokaler Server
Nur Computer aus Ihrem lokalen Netzwerk können sich als Server mit Ihrem Mac verbinden. Sie haben weiterhin Zugriff auf das Internet.

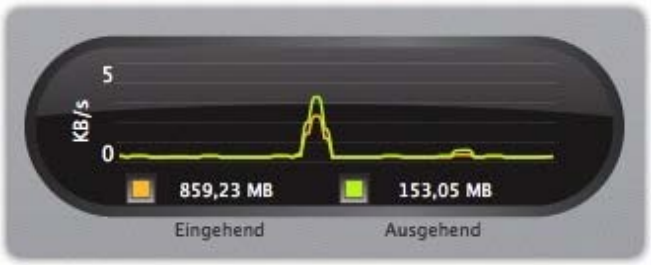
Die erste Anzeige der mittleren Gruppe informiert Sie darüber, ob der Anti-Phishing-Schutz aktiviert ist. "Phishing" ist eine Art von Angriff, bei dem Cyber-Kriminelle versuchen, Sie auszutricksen, um an Ihre privaten Informationen (z.B. Finanzdaten oder ein Passwort) zu gelangen. Auf diese Weise erhalten diese Leute Zugriff auf Ihre persönlichen Daten, wie z.B. Zugangsdaten für Ihre E-Mail- oder sogar für Ihre Bankkonten. Wenn Sie auf diese Schaltfläche klicken wird ein Fenster geöffnet, in dem Sie Seiten hinzufügen können, denen Sie vertrauen, und die daher vom Anti-Phishing-Schutz ausgenommen werden sollen. (Sie können auf dieses Fenster auch zugreifen, indem Sie auf die große Schaltfläche "Surfen" oben im Fenster und dann auf die Registerkarte "Anti-Phishing" klicken.)



Die zweite Anzeige in dieser Gruppe informiert Sie darüber, ob der Web Threat-Schutz aktiviert ist. Wenn Sie auf diese Schaltfläche klicken wird ein Fenster geöffnet, in dem Sie Seiten hinzufügen können, denen Sie vertrauen, und die daher vom Web Threat-Schutz ausgenommen werden sollen. (Sie können auf dieses Fenster auch zugreifen, indem Sie auf die große Schaltfläche "Surfen" oben im Fenster und dann auf die Registerkarte "Web Threats" klicken.)

Die untere Anzeige in dieser Gruppe zeigt die Anzahl von Adressen an, die gesperrt wurden und die nicht mit Ihrem Computer kommunizieren dürfen. Diese Adressen sind entweder gesperrt, weil VirusBarrier X6 sie als schädlich eingestuft hat oder weil sie von Ihnen manuell hinzugefügt wurden. Wenn Sie auf diese Schaltfläche klicken wird ein Fenster geöffnet, das Ihnen anzeigt, welche Adressen gesperrt wurden sowie Details darüber, warum sie gesperrt wurden und wie lange sie noch gesperrt sind. (Sie können auf dieses Fenster auch zugreifen, indem Sie auf die große Schaltfläche "Antivandalismus" oben im Fenster und dann auf die Registerkarte "Gesperrte Adressen" klicken.)

Die letzte Anzeige in der Spalte für den Netzwerkschutz ist die Anzeige für den Netzwerk-Datenverkehr. Sie wird in Echtzeit aktualisiert und zeigt an, wie viele Daten auf Ihrem Computer ein- und ausgehen. Bei dieser Anzeige handelt es sich nicht um eine Schaltfläche. Es passiert daher nichts, wenn Sie darauf klicken. Wenn Sie weitere Informationen über den Netzwerkdatenverkehr wünschen, klicken Sie auf die Schaltfläche für die Datenverkehrsüberwachung in der unteren rechten Ecke des Fensters.

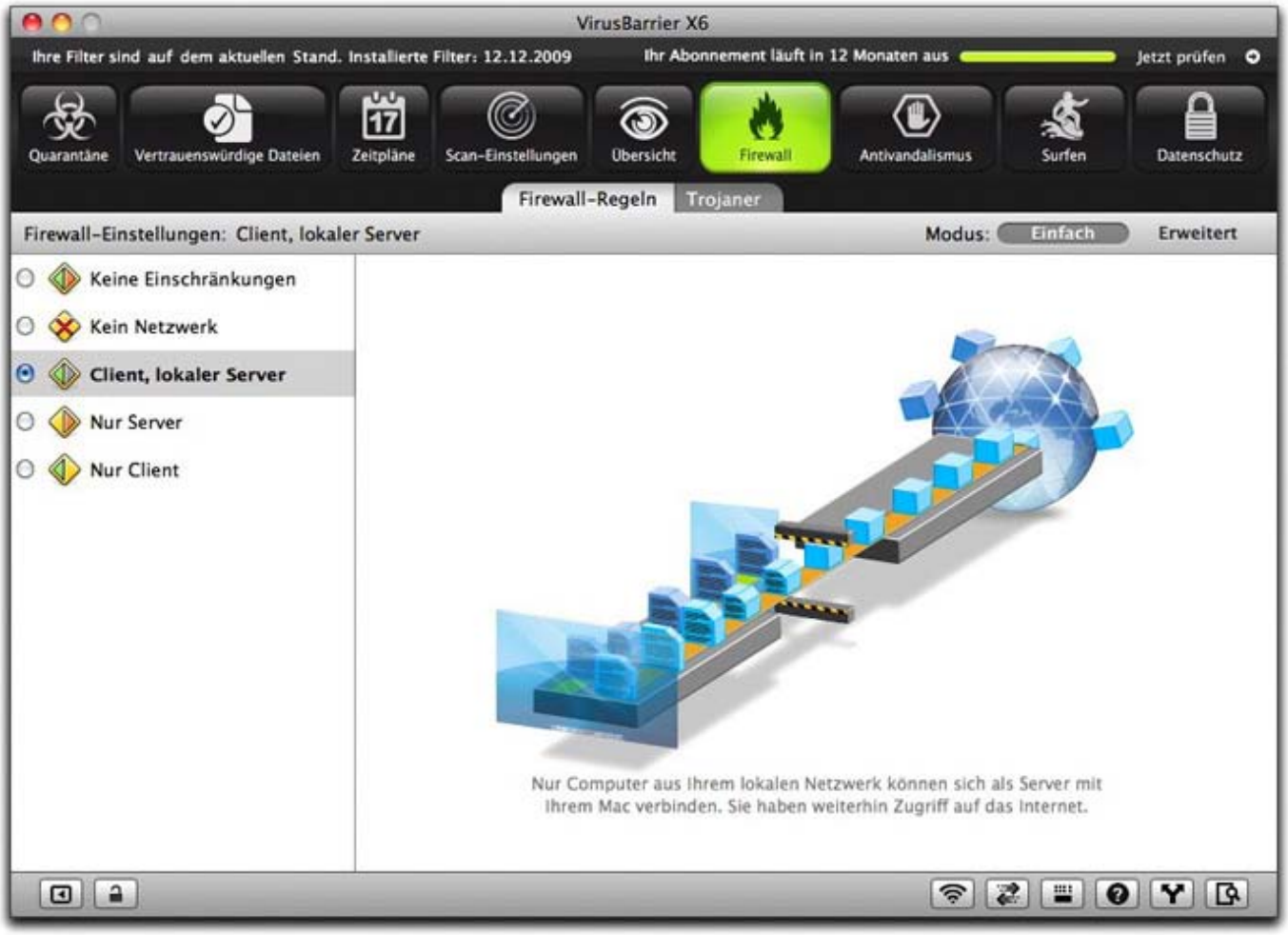


Firewall-Schutz

VirusBarrier X6 enthält eine persönliche Firewall. Dabei handelt es sich um eine leistungsstarke Funktion, die alle Datenpakete filtert, die auf Ihrem Mac über das Internet oder ein lokales TCP/IP-Netzwerk ein- und ausgehen. Die Firewall schützt auch vor Trojanischen Pferden, indem die von diesen verwendeten Ports gesperrt werden.

Wenn Sie die Firewall-Einstellungen ansehen oder ändern möchten, klicken Sie auf die Schaltfläche "Firewall".

Wenn Sie auf die Schaltfläche "Firewall" klicken, zeigt VirusBarrier X6 den einfachen Modus für die Steuerung der Firewall-Einstellungen an. Es gibt fünf voreingestellte Firewall-Konfigurationen, die alle Situationen abdecken, die bei normaler Verwendung eintreten können. Jede Einstellung wird von einer Animation begleitet, die grafisch anzeigt, welche Auswirkungen die Anwendung der Einstellung hat. Das Fenster direkt vor Ihnen repräsentiert Ihren Mac. Der Globus steht für das Internet und das Fenster zwischen den beiden repräsentiert die Grenzen Ihres lokalen Netzwerks. Die Standardeinstellung hier ("Client, lokaler Server") zeigt an, dass Ihr Computer Informationen von außerhalb des lokalen Netzwerks empfangen kann, aber die Computer außerhalb Ihres lokalen Netzwerks können nicht auf Ihren Mac zugreifen.



Es gibt folgende fünf Firewall-Einstellungen:

- **Keine Einschränkungen**: Die Firewall von VirusBarrier X6 erlaubt das Senden und Empfangen aller ein- und ausgehenden Netzwerkdaten.
- **Kein Netzwerk**: Die Firewall von VirusBarrier X6 sperrt den Empfang und den Versand sämtlicher Daten aus einem und in ein lokales TCP/IP-Netzwerk bzw. aus dem/ins Internet. Dieser Modus ermöglicht es Ihnen, jeden Netzwerk-Datenverkehr Ihres Computers zu sperren, wenn Sie beispielsweise nicht an Ihrem Computer sitzen.
- **Client, lokaler Server**: Die Firewall von VirusBarrier X6 erlaubt die Verwendung Ihres Mac als Client und als lokalen Netzwerkserver. Ihr Mac kann als Client-Computer auf das Internet zugreifen und Ihr Mac kann sowohl als Client als auch als Server in einem lokalen Netzwerk dienen.
- **Nur Server**: Die Firewall von VirusBarrier X6 erlaubt nur die Verwendung Ihres Mac als Server: alle Client-Funktionen, einschließlich der Fähigkeit im Internet zu surfen, sind blockiert.
- **Nur Client**: Die Firewall von VirusBarrier X6 erlaubt nur die Verwendung Ihres Mac als Client in einem lokalen Netzwerk oder im Internet. Die Server- und Filesharing-Funktionen Ihres Mac sind gesperrt.

Diese fünf Einstellungen sind für die meisten Leute ausreichend. Wenn Sie jedoch mehr Kontrolle über den Zugriff auf Ihren Computer möchten, wenn Sie beispielsweise eine Spieleparty durchführen und den gesamten Datenverkehr verbieten möchten, außer der Kommunikation zwischen den Spielteilnehmern, müssen Sie in den erweiterten Modus von VirusBarrier X6 wechseln.

Erweiterter Modus

VirusBarrier X6 bietet auch einen erweiterten Firewall-Modus, in dem Sie Ihre eigenen Regeln erstellen und so genau auswählen können, welche Arten von ein- und ausgehendem Datenverkehr Sie auf Ihrem Mac zulassen oder verbieten

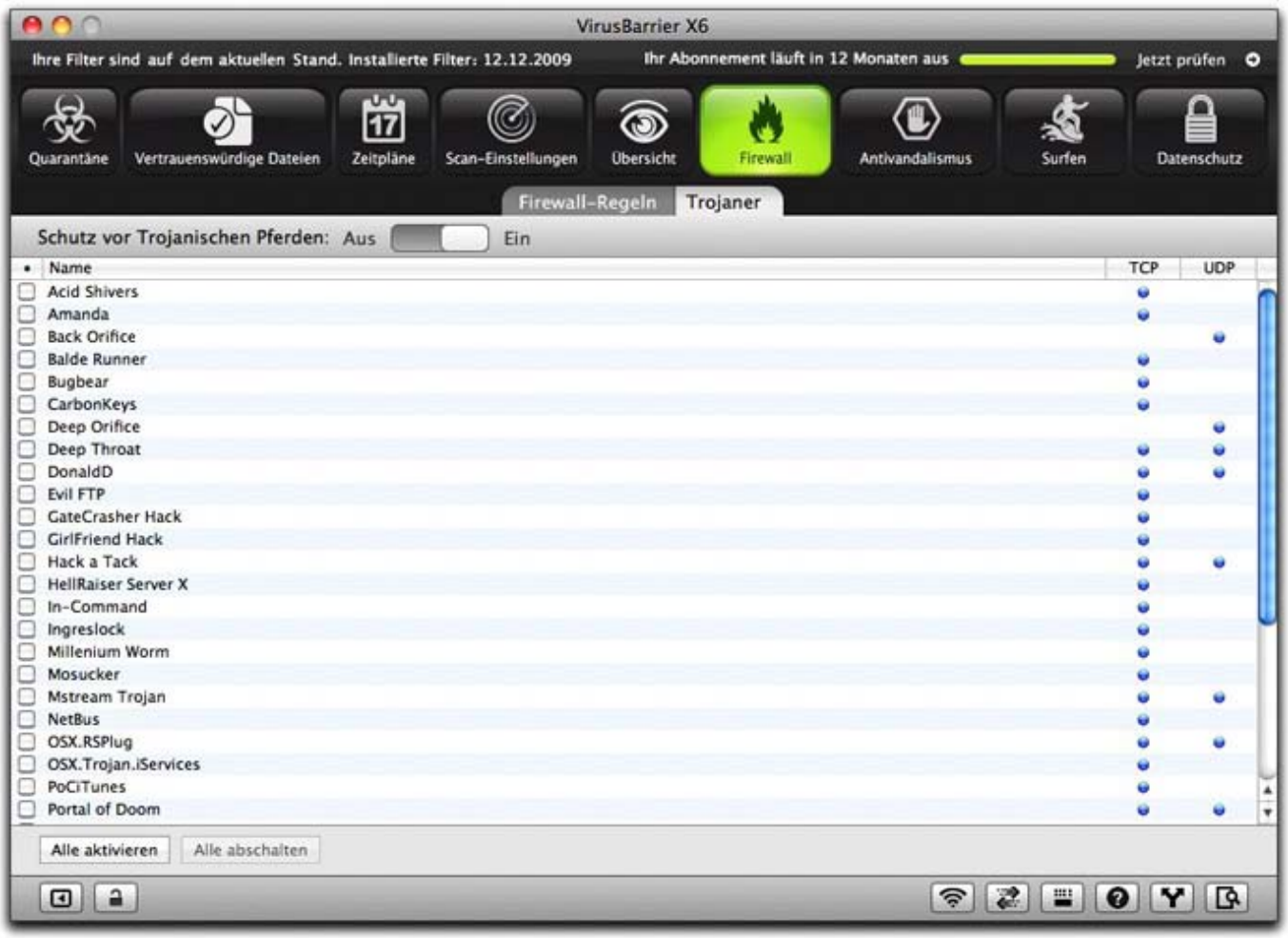
möchten. Weitere Informationen über die Verwendung des erweiterten Modus finden Sie unter Anhang: So erstellen Sie eigene Firewall-Regeln.

Schutz vor Trojanischen Pferden

Trojanische Pferde sind Programme, die ohne Ihr Wissen auf Ihrem Computer installiert werden. Das passiert entweder durch Anhänge, die Sie per E-Mail erhalten, oder durch Programme, die Sie von betrügerischen Websites herunterladen. In manchen Fällen installieren Programme eine bestimmte Art von Trojanischem Pferd. Diese als Spyware bezeichnete Software sendet persönliche Informationen an einen Server. Da die Verbindung *von* Ihrem Computer hergestellt wird, gilt sie generell als vertrauenswürdig.

VirusBarrier X6 kann die Aktivitäten der meisten bekannten Trojanischen Pferde entdecken und stoppen. Einige dieser Programme senden Informationen über das Surfverhalten des Benutzers an einen zentralen Server. Andere Trojanische Pferde öffnen "Hintertüren" auf Ihrem Computer. So können sich Hacker die Kontrolle über Ihren Computer verschaffen oder Dateien stehlen. Zudem erkennt VirusBarrier X6 die Aktionen von Trojanischen Pferden für Windows. Wenn Sie also Windows in einer virtuellen Umgebung ausführen (z.B. mit einem Programm wie VMware Fusion oder Parallels Desktop) und die Internetverbindung Ihres Mac im NAT-Modus gemeinsam verwenden, sind Sie geschützt.

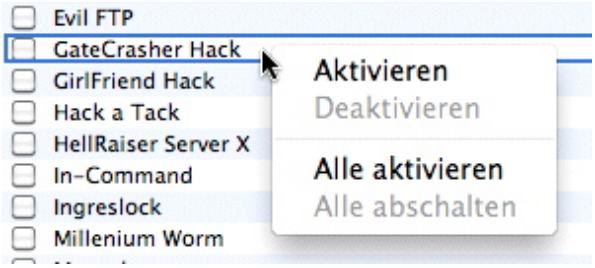
Klicken Sie auf die Registerkarte "Trojaner" oben im Firewall-Fenster, um sich die Bedienelemente von VirusBarrier X6 für Trojanische Pferde anzeigen zu lassen.



Sie können den Schutz vor Trojanischen Pferden aktivieren, indem Sie den Schieberegler für den Schutz vor Trojanischen Pferden auf "Ein" schieben. Nun müssen Sie noch auf die Kontrollkästchen für die einzelnen Trojanischen Pferde klicken, vor denen Ihr Computer geschützt werden soll. Die Schaltflächen zum Aktivieren und Deaktivieren aller

Optionen am unteren Rand können Sie als praktische Kurzbefehle verwenden, um alle Kontrollkästchen auf einmal auszuwählen oder um die gesamte Auswahl auf einmal aufzuheben.

Sie können den Schutz vor Trojanischen Pferden auch nur für ein einzelnes Trojanisches Pferd oder für alle Trojanischen Pferde aktivieren. Klicken Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf den Namen des betreffenden Trojanischen Pferds und wählen Sie den entsprechenden Befehl aus dem Kontextmenü, das daraufhin angezeigt wird.

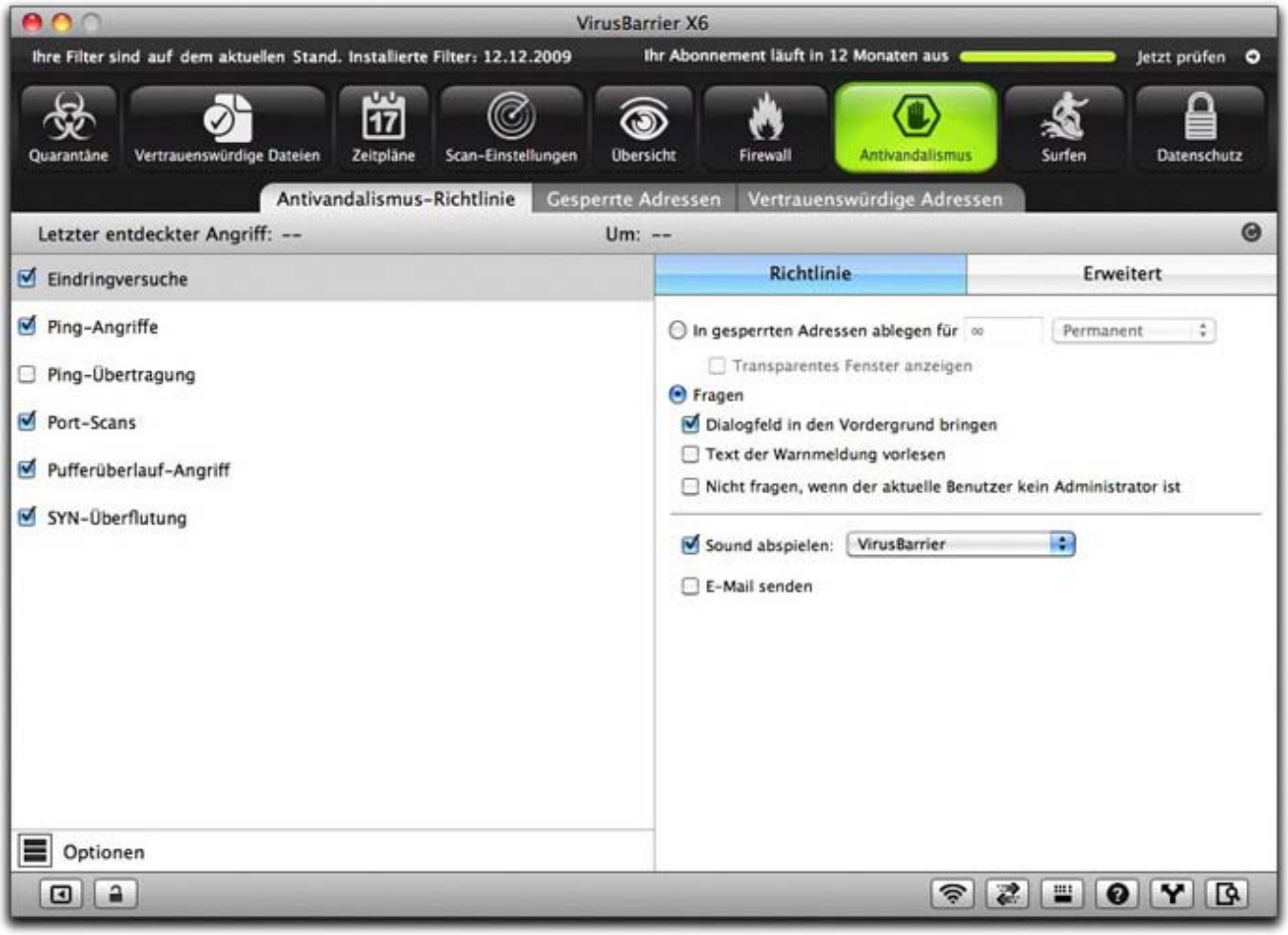


Antivandalismus-Schutz

Dank seiner integrierten Funktion "Antivandalismus" ist VirusBarrier X6 in der Lage, die bei Ihrem Mac eingehenden Datenpakete daraufhin zu überwachen, ob jemand versucht, in Ihren Mac einzudringen. Bei Bedarf werden diese eingehenden Datenpakete gefiltert. Diese Filterung ist transparent: Sie werden nur dann Zeichen dafür erkennen, dass sie funktioniert, wenn verdächtige Daten erkannt werden. In diesem Fall wird eine Warnmeldung angezeigt. Ansonsten überwacht die Funktion "Antivandalismus" kontinuierlich alle Netzwerkaktivitäten Ihres Mac im Hintergrund.

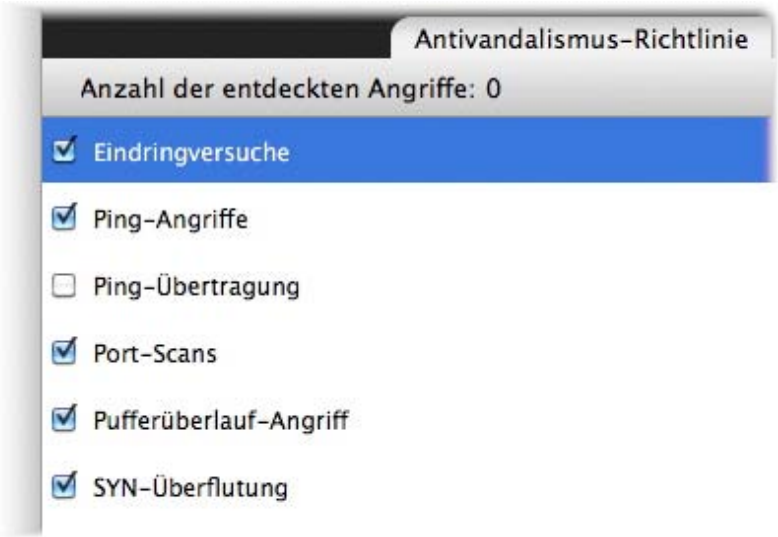
Klicken Sie auf die Schaltfläche "Antivandalismus" um das Fenster "Antivandalismus" zu öffnen.

Die Registerkarte "Antivandalismus-Richtlinie" steuert, wie auf Ihrem Computer eingehende Daten gefiltert werden. Die Registerkarten "Gesperrte Adressen" und "Vertrauenswürdige Adressen" speichern bestimmte Hosts oder IP-Adressen, die Sie für verdächtig oder vertrauenswürdig halten.



Antivandalismus-Richtlinie

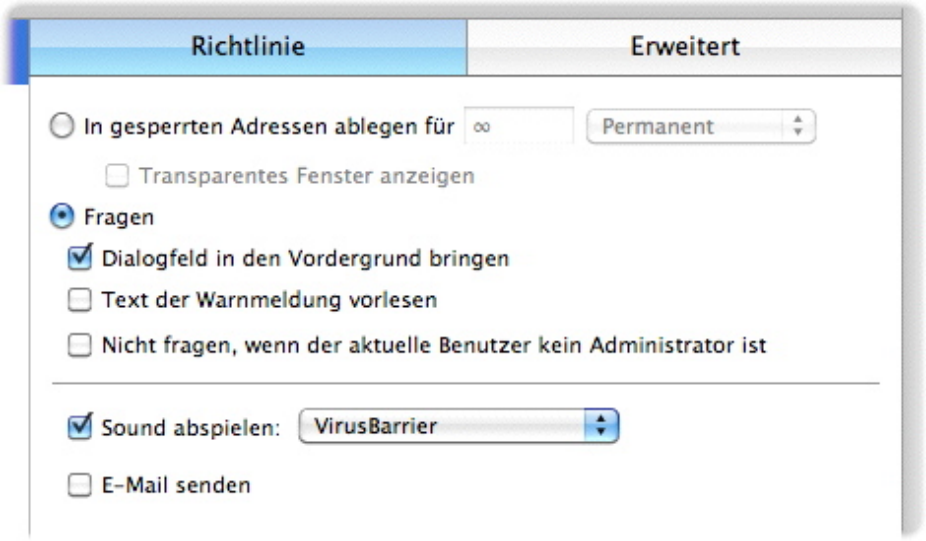
Der Fensterabschnitt "Antivandalismus-Richtlinie" bietet Tools, die vor sechs Arten des Eindringens schützen.



- **Pufferüberlauf-Angriff**: Diese Angriffe können auftreten, wenn eine bestimmte Software Fehler beim Umgang mit Speicherplatz aufweist und Benutzern mit bösen Absichten so den Zugriff auf Ihren Mac erlaubt.
- **Eindringversuche**: Versuche auf Ihren Mac über eine voreingestellte Anzahl von falschen Passwortanfragen innerhalb eines bestimmten Zeitraum zuzugreifen. Es gibt verschiedene Einstellungen für AppleShare IP (ASIP), FTP, HTTP, IMAP, POP und SMTP.

- **Ping-Angriffe**: Ihr Mac empfängt eine so große Anzahl oder Frequenz von Pinganfragen, das eine Beantwortung Ihren Mac überlasten würde.
- **Ping-Übertragungsangriffe**: Pinganfragen zur Übertragung von Adressen, wobei ein einzelner Ping über Ihr lokales Netzwerk vervielfacht wird.
- **Port-Scans**: Versuche von Remote-Computern, die Ports Ihres Mac auf Schwachstellen zu prüfen. Wenn Sie Ihren Computer als Server einsetzen, ist es unter Umständen besser, dieses Kontrollkästchen nicht zu markieren.
- **SYN-Überflutung**: Mehrere TCP-Anfragen, die von einem Angreifer gesendet werden, der den letzten Schritt des Austausches dann nicht vollzieht. So verbraucht der Zielcomputer Ressourcen.

Wenn Sie auf das Kontrollkästchen neben diesen Optionen klicken, wird der Schutz vor dieser Art des Eindringens aktiviert oder deaktiviert. Wenn Sie auf den Namen für den Eindringtyp klicken, werden die Richtlinien für die Benachrichtigung und die Aktion für diese Art des Eindringens angezeigt. Die folgende Abbildung zeigt beispielsweise die Richtlinie für Pufferüberlauf-Angriffe.



Diese Optionen werden weiter hinten in diesem Kapitel unter Die Bedeutung von Warnmeldungen ausführlich erklärt.

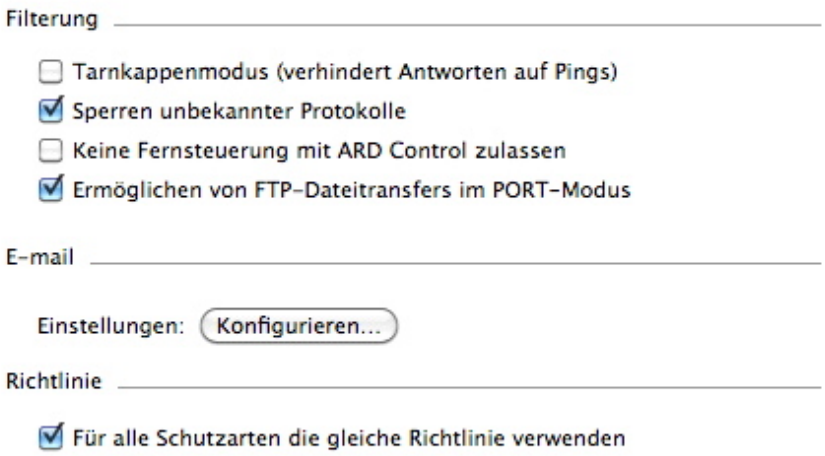
Wenn Sie auf die Registerkarte "Erweitert" im rechten Fensterabschnitt klicken, während ein Eindringtyp ausgewählt ist, werden weitere Optionen speziell für diesen Eindringtyp angezeigt. Hierzu zählen:

- **Pufferüberlauf-Angriff**: Keine erweiterten Einstellungen.
- **Eindringversuche**: Sie können die Anzahl erlaubter falscher Passworteingaben für AppleShare IP (ASIP), FTP, HTTP, IMAP, POP und SMTP getrennt eingeben.
- **Ping-Angriffe**: Die Sensibilität für Ping-Überflutung, gemessen in Millisekunden (ms), die zwischen Ping-Versuchen erlaubt ist. Wenn Ihr Computer in ein Netzwerk integriert ist, ist es vollkommen normal, dass der Netzwerkverwalter Ihren Computer gelegentlich per Ping "anbimmelt". Andernfalls sind Pings jedoch seltener. Die einzige Ausnahme hiervon dürfte der Fall sein, wenn Sie Ihren Computer über ein DSL- oder Kabelmodem mit dem Internet verbunden haben und Ihr ISP Ihrem Computer ab und zu eine Ping-Anfrage sendet, um zu prüfen, ob Ihr Computer mit dem Kabelnetzwerk verbunden ist.
- **Ping-Übertragungsangriffe**: Keine erweiterten Einstellungen.
- **Port-Scans**: Die Sensibilität ist mit einem Schieberegler von niedrig bis hoch einstellbar. Die Intervalle entsprechen einer internen Berechnung.
- **SYN-Überflutung**: Sensibilität, die in der Anzahl von Verbindungsversuchen gemessen wird, die pro Sekunde erlaubt sind.

Optionen

Klicken Sie auf die Schaltfläche "Optionen" in der unteren linken Ecke des Fensters "Antivandalismus-Richtlinie", um weitere Filtereinstellungen anzupassen.

Die Optionen werden im Fensterabschnitt rechts angezeigt.



- **Tarnkappenmodus ("stealth mode"; verhindert Antworten auf Pings)**: Wenn dieses Kontrollkästchen markiert ist, bleibt Ihr Computer für andere Computer im Internet oder in einem lokalen Netzwerk unsichtbar. Allerdings bleiben Sie nicht anonym: alle von Ihren Computer gesendeten Anfragen werden mit der IP-Nummer Ihres Computers identifiziert.
- **Sperren unbekannter Protokolle**: Wenn dieses Kontrollkästchen markiert ist, blockiert VirusBarrier X6 automatisch alle unbekannten Protokolle.
- **Keine Fernsteuerung mit ARD Control erlauben**: Wenn dieses Kontrollkästchen markiert ist, sperrt VirusBarrier X6 alle Aktivitäten von Apple Remote Desktop.
- **Ermöglichen von FTP-Dateitransfers im PORT-Modus**: Wenn dieses Kontrollkästchen markiert ist, können Sie FTP-Dateitransfers durchführen, wenn Ihr Computer im Firewall-Modus "Nur Client" arbeitet.

Im zweiten Teil dieses Fensters können Sie sich per E-Mail benachrichtigen lassen, wenn ein Angriff entdeckt wird. Weitere Informationen hierzu erhalten Sie weiter hinten in diesem Kapitel unter Die Bedeutung von Warnmeldungen.

Vereinheitlichen der Optionen für alle Richtlinien

Für jede Art des Eindringens gibt es Einstellungen, mit denen Sie festlegen können, wie Sie gewarnt werden und welche Aktionen ausgeführt werden sollen, wenn diese Art des Eindringens entdeckt wird.

Das Kontrollkästchen "Für alle Schutzarten die gleiche Richtlinie verwenden" vereinheitlicht alle Benachrichtigungen und Aktionen. Wenn dieses Kontrollkästchen nicht markiert ist, könnten Sie beispielsweise Folgendes auswählen: Sie erhalten eine E-Mail, wenn ein Pufferüberlauf-Angriff entdeckt wird. Wenn jedoch ein Eindringversuch stattfindet, wird Ihnen nur eine Warnmeldung anzeigt. Wenn Sie das Kästchen markieren, liefert Ihnen VirusBarrier X6 bei jeder Art des Eindringens die gleiche Antwort.

Wenn Sie diese Option einschalten, wird Ihnen ein Dialogfeld angezeigt, in dem Sie die Mustereinstellungen auswählen können, die alle weiteren Eindringtypen übernehmen sollen.

Gesperrte Adressen und Vertrauenswürdige Adressen

Die Liste mit gesperrten Adressen garantiert, dass die Datenübertragung zwischen dem Gerät eines Angreifers und Ihrem Mac, nachdem ein versuchter Angriff oder ein Eindringversuch verhindert wurde, für den von Ihnen festgelegten Zeitraum unterbunden wird.

Die Liste mit vertrauenswürdigen Adressen ist das Gegenteil der Liste mit gesperrten Adressen: Sie führt "befreundete" Computer auf, denen eine Verbindung mit Ihrem Mac *erlaubt* wird. Während die Liste mit gesperrten Adressen Sie vor "Feinden" schützt, öffnet die Liste mit vertrauenswürdigen Adressen Ihren Freunden die Tür. Die Antivandalismus-Funktion von VirusBarrier X6 sperrt den Zugriff auf Computer in der Liste mit vertrauenswürdigen Adressen nicht und gibt auch keine Warnmeldungen über irgendwelche Aktionen aus, die von ihnen ausgeführt werden. Alle aktiven Firewall-Regeln werden jedoch auch auf die Computer in der Liste mit vertrauenswürdigen Adressen angewendet.

Die Oberfläche des Fensters für die "Vertrauenswürdigen Adressen" sieht im Prinzip genauso aus, wie das Fenster für "Gesperrten Adressen". Wir untersuchen daher beide gemeinsam und heben die wichtigen Unterschiede hervor. Hier eine Abbildung des Fensters für gesperrte Adressen.

Im linken Fensterabschnitt werden Informationen über die verschiedenen IP-Adressen angezeigt, die derzeit in der Liste mit gesperrten Adressen oder in der Liste mit vertrauenswürdigen Adressen gespeichert sind - sofern es dort welche gibt.

- **Kontrollkästchen**: Sie können ein Element der Liste mit gesperrtenvertrauenswürdigen Adressen vorübergehend deaktivieren, indem Sie das Häkchen aus diesem Kontrollkästchen entfernen. Es wird standardmäßig aktiviert, wenn Sie einen Host auf eine der beiden Listen setzen. Wenn ein Element deaktiviert ist, wird es wieder aktiviert, wenn Sie darauf klicken. (Dieses Kontrollkästchen wird nur angezeigt, wenn die IP-Adresse so eingestellt ist, dass sie dauerhaft gesperrt wird.)
- **Eindringling/Host**: Die zweite Spalte zeigt die eindringende IP-Adresse (in der Liste mit gesperrten Adressen) oder die erlaubte IP-Adresse (in der Liste mit vertrauenswürdigen Adressen) an.
- **Verbleibende Zeit**: Wenn Sie eingestellt haben, dass diese IP-Adresse für einen bestimmten Zeitraum gesperrt oder zugelassen werden soll, wird in dieser Spalte angezeigt, wie viel Zeit noch verbleibt. Die Anzeige wird jede Sekunde aktualisiert. Andernfalls wird in dieser Spalte "Permanenter Host" angezeigt. Das heißt, die IP-Adresse bleibt solange dort, bis Sie sie manuell entfernen.

Informationen über gesperrte/vertrauenswürdige Adressen

Wenn Sie auf ein Element in der Liste mit gesperrten/vertrauenswürdigen Adressen klicken, werden in der rechten Hälfte des Fensterabschnitts weitere Informationen angezeigt. Wenn Sie auf das Element doppelklicken, wird ein neues Fenster mit den gleichen Informationen geöffnet.

- **Host**: Die IP-Adresse des Servers. Wenn Sie ein neues Fenster geöffnet haben, indem Sie auf das Element doppelgeklickt haben, können Sie die aufgeführte IP-Adresse manuell ändern. Wenn Sie auf das Fragezeichensymbol (**?**) zum Starten von DNS-Anfragen (DNS, Domain Name Server = Domänennamen-Server) klicken, können Sie von der Anzeige der IP-Nummer des Angreifers auf die Anzeige seines Domänennamens umschalten, sofern dieser bekannt ist. Sie können sich diese Adresse in großer Schrift anzeigen lassen. Verschieben Sie hierzu den Mauszeiger über das Wort "Host". Klicken Sie mit der Maus darauf und wählen Sie aus dem Kontextmenü die Option "Große Schrift".
- **Grund**: Weshalb die IP-Nummer in die Liste mit gesperrten Adressen aufgenommen wurde. Dieser Text wird nicht im Fenster für die Liste mit vertrauenswürdigen Adressen angezeigt, da alle Elemente dort manuell hinzugefügt werden.
- **Gesamtzeit**: Die Zeit, die eine Internet-Adresse eines anderen Computers in der Liste mit gesperrten/vertrauenswürdigen Adressen verbleibt. Wenn Sie auf das Wort "Gesamtzeit" klicken, wird die Anzeige geändert und gibt die verbleibende Zeit an. Wenn Sie noch einmal darauf klicken wird die abgelaufene Zeit angezeigt. Sie gibt darüber Auskunft, wie lange der Angreifer bereits auf der Liste mit gesperrten Adressen steht. Wenn Sie auf "Abgelaufene Zeit" klicken, wird Ihnen noch einmal die Gesamtzeit angezeigt.
- **Ankunft**: Wann die IP-Nummer in die Liste mit gesperrten Adressen aufgenommen wurde.
- **Start**: Wenn Sie für eine IP-Adresse einen Zeitraum festgelegt haben, über den diese in der Liste mit gesperrten/vertrauenswürdigen Adressen verbleiben soll, wird an dieser Stelle der Zeitpunkt angegeben, an dem sie wieder gelöscht wird.
- **Anmerkung**: Alle Anmerkungen, die Sie für diese IP-Adresse eingegeben haben. VirusBarrier X6 fügt zudem automatisch Anmerkungen hinzu, wenn das Programm ein Element in die Liste mit gesperrten Adressenaufnimmt (wie im obigen Beispiel).

Hinweis zum Überprüfen der DNS

An mehreren Stellen auf der Oberfläche von VirusBarrier X6 wird Ihnen ein Fragezeichen in einem dunklen Kreis angezeigt. Wenn Sie darauf klicken, können Sie sich für eine numerische IP-Adresse den zugehörigen Domänennamen anzeigen lassen und umgekehrt.

Beachten Sie bitte, dass IP-Adressen nicht immer eine eindeutige Beziehung zu Domänennamen haben. Eine große Domäne kann beispielsweise "www.beispiel.com" auf einer IP-Adresse hosten, "foren.beispiel.com" auf einer anderen und "blog.beispiel.com" wiederum auf einer anderen.

Kleine Domänen wiederum teilen sich eine IP-Adresse oft mit anderen, wobei alle als "virtuelle Domänen" auf einem einzigen Computer gehostet sind. In solchen Fällen erhalten Sie beim Überprüfen einer Domäne eine IP-Adresse, die tatsächlich zu einem größeren, unerwarteten Gerätenamen führt, beispielsweise "apache2-vat.market.beispiel.com".

Das kann dazu führen, dass durch das Eingeben einer IP-Adresse der Datenverkehr von unbeabsichtigten Domänen gesperrt (oder erlaubt) wird, während das Eingeben einer Domäne möglicherweise nicht den gesamten gewünschten

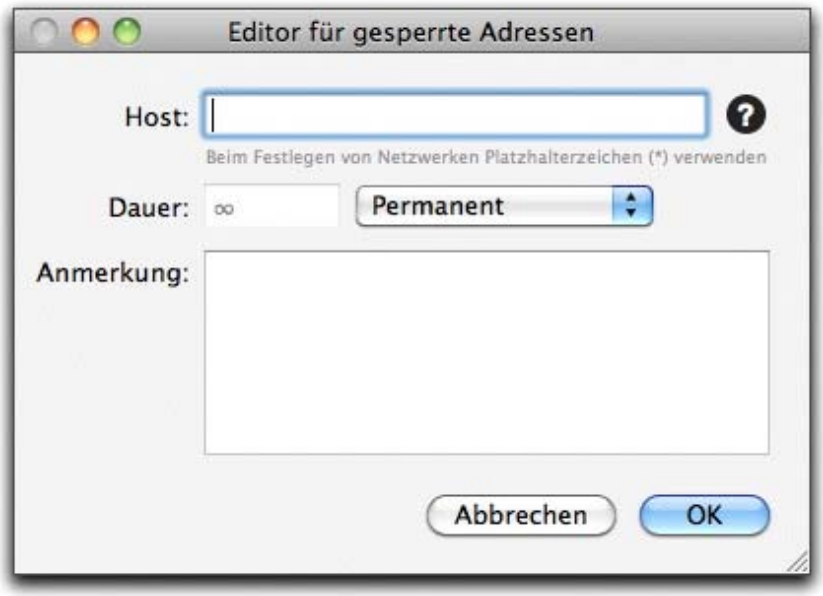
Datenverkehr sperrt (oder erlaubt). Das liegt an der Beschaffenheit der Internetdomänenstruktur und ist kein Fehler von VirusBarrier X6. Wenn Sie Probleme damit haben, dass Datenverkehr unerwartet gesperrt oder zugelassen wird, versuchen Sie an Stelle einer IP-Adresse einen Domänennamen zu verwenden und umgekehrt.

So fügen Sie Adressen hinzu

Sie können Adressen manuell auf zwei Arten zur Liste mit gesperrten Adressen oder zur Liste mit vertrauenswürdigen Adressen hinzufügen. (VirusBarrier X6 kann Adressen auch automatisch als Reaktion auf Warnmeldungen zur Liste mit gesperrten Adressen hinzufügen. Weitere Informationen erhalten weiter hinten in diesem Kapitel unter Die Bedeutung von Warnmeldungen.)

Die erste Möglichkeit der Liste mit gesperrten Adressen oder der Liste mit vertrauenswürdigen Adressen eine Adresse hinzuzufügen besteht darin, eine IP-Adresse aus dem Protokollfenster zu wählen und dann im Kontextmenü die Option "Zu gesperrten Adressen hinzufügen" oder "Zu vertrauenswürdigen Adressen hinzufügen" zu wählen. Weitere Informationen hierzu finden Sie unter So verwenden Sie die Überwachungstools von VirusBarrier X6.

Sie können Adressen auch manuell der Liste mit gesperrten/vertrauenswürdigen Adressen hinzufügen, indem Sie auf das Pluszeichen (+) am unteren Rand der Liste klicken. Daraufhin wird ein Fenster angezeigt.

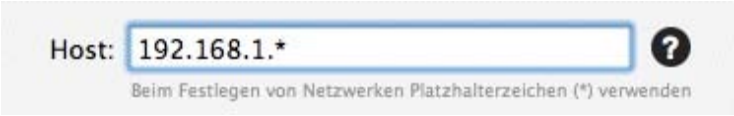


Geben Sie in das Feld "Host:" eine IP-Adresse ein. Wählen Sie, über welchen Zeitraum diese in der Liste mit gesperrten Adressen oder in der Liste mit vertrauenswürdigen Adressen gespeichert bleiben soll, indem Sie in das Feld "Dauer" eine entsprechende Zahl eingeben. Wählen Sie dann eine Zeiteinheit aus dem Popup-Menü. Wenn Sie die numerische IP-Adresse des anderen Computers, den Sie hinzufügen möchten, nicht kennen, müssen Sie seinen Domänennamen eingeben und auf die Schaltfläche mit dem Fragezeichen **?** klicken. VirusBarrier X6 fragt nun den DNS-Server Ihres ISP (Internet Service Provider = Internet-Dienstleister) an und trägt die korrekte IP-Nummer in das Feld ein. In das Feld "Anmerkung:" können Sie auch Anmerkungen wie z.B. den Grund für die Aufnahme der Internet-Adresse eingeben. Wenn Sie die Internet-Adresse nicht in die Liste mit gesperrten Adressen oder in die Liste mit vertrauenswürdigen Adresseneingeben wollen, klicken Sie auf "Abbrechen".

So verwenden Sie Platzhalterzeichen

Sie können Platzhalterzeichen verwenden, um Bereiche von IP-Nummern in der Liste mit gesperrten Adressen oder in der Liste mit vertrauenswürdigen Adressen festzulegen. Geben Sie hierzu den ersten Teil der IP-Adresse ein, den Sie sperren möchten und geben Sie anschließend Sternchen ein. Die Nummer 192.168.1.* sperrt beispielsweise alle IP-Adressen von 102.168.1.0 bis einschließlich 192.168.1.255. Die Nummer 192.168.*.* sperrt IP-Adressen von

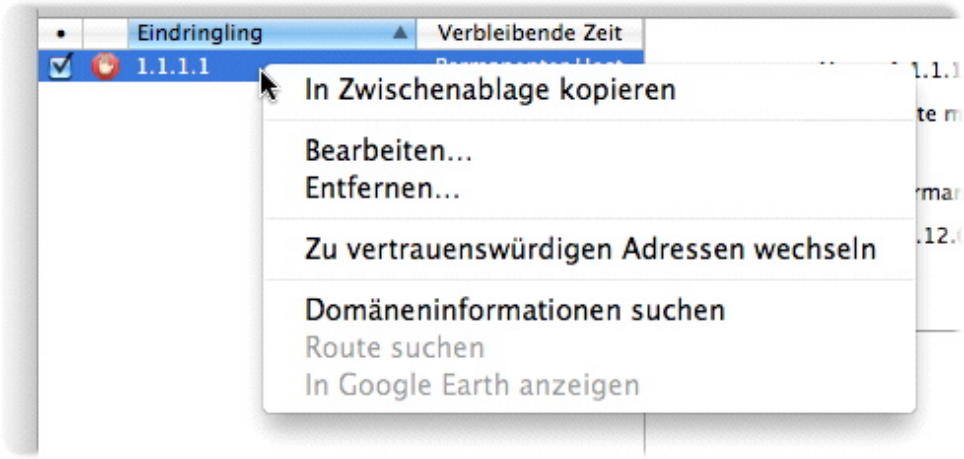
192.168.[0-255].[0-255] usw.



So entfernen oder verschieben Sie Adressen

Wenn Sie eine Internet-Adresse aus der Liste mit gesperrten Adressen oder aus der Liste mit vertrauenswürdigen Adressen löschen wollen, klicken Sie auf die betreffende Internet-Adresse und dann auf das Minuszeichen. Daraufhin müssen Sie in einem Dialogfeld bestätigen, dass Sie die Internet-Adresse wirklich löschen wollen.

Sie können eine Internet-Adresse auch löschen, indem Sie die Steuerungstaste auf Ihrer Tastatur gedrückt halten, auf die betreffende Internet-Adresse klicken und dann aus dem Kontextmenü die Option "Entfernen..." wählen. Daraufhin müssen Sie in einem Dialogfeld bestätigen, dass Sie die Internet-Adresse wirklich löschen wollen. Über dieses Kontextmenü können Sie die Adresse auch von der Liste mit gesperrten Adressen in die Liste mit vertrauenswürdigen Adressen verschieben und umgekehrt.



So bearbeiten Sie eine Adresse

Sie können Adressen auf drei Arten in der Liste mit gesperrten Adressen oder in der Liste mit vertrauenswürdigen Adressen bearbeiten:

- Klicken Sie auf die Adresse, die Sie bearbeiten möchten, klicken Sie dann auf die Schaltfläche "Bearbeiten" am unteren linken Rand des Fensterabschnitts.
- Doppelklicken Sie auf die Adresse oder
- klicken Sie auf die Adresse während Sie die Steuerungstaste auf Ihrer Tastatur gedrückt halten. Wählen Sie dann "Bearbeiten..." aus dem Kontextmenü.

Daraufhin wird das Editor-Fenster für gesperrte/vertrauenswürdige Adressen angezeigt. Sie können die Adresse ändern, Anmerkungen hinzufügen oder bearbeiten oder den Zeitraum ändern, über den das Element in der Liste mit gesperrten/vertrauenswürdigen Adressen verbleiben soll.

Das Kontextmenü

Wie Sie bereits gesehen haben, können Sie bei gedrückter Taste "ctrl" auf der Tastatur Ihres Macintosh auf eine Internet-Adresse in der Liste mit gesperrten/vertrauenswürdigen Adressen klicken. Hierauf wird ein Kontextmenü geöffnet. In diesem Menü gibt es vier Funktionen, die noch nicht erklärt wurden: In Zwischenablage kopieren, Domäneninformationen suchen, Route suchen und In Google Earth anzeigen.

- **In Zwischenablage kopieren**: Kopiert die IP-Adresse in die Zwischenablage von Mac OS X. Von dort aus kann sie in andere Programme eingefügt werden (z.B. in ein Texbearbeitungsprogramm).
- **Domäneninformationen suchen**: Öffnet das Whois-Fenster von VirusBarrier X6 und führt eine Suche nach der ausgewählten IP-Adresse durch. Siehe So verwenden Sie die Überwachungstools von VirusBarrier X6.
- **Route suchen**: Öffnet das Traceroute-Fenster von VirusBarrier X6 und führt eine Suche nach der ausgewählten IP-Adresse durch. Siehe So verwenden Sie die Überwachungstools von VirusBarrier X6.
- **In Google Earth anzeigen**: Startet das Programm Google Earth, sofern Sie es installiert haben, und versucht, den geografischen Ort der ausgewählten IP-Adresse zu finden.

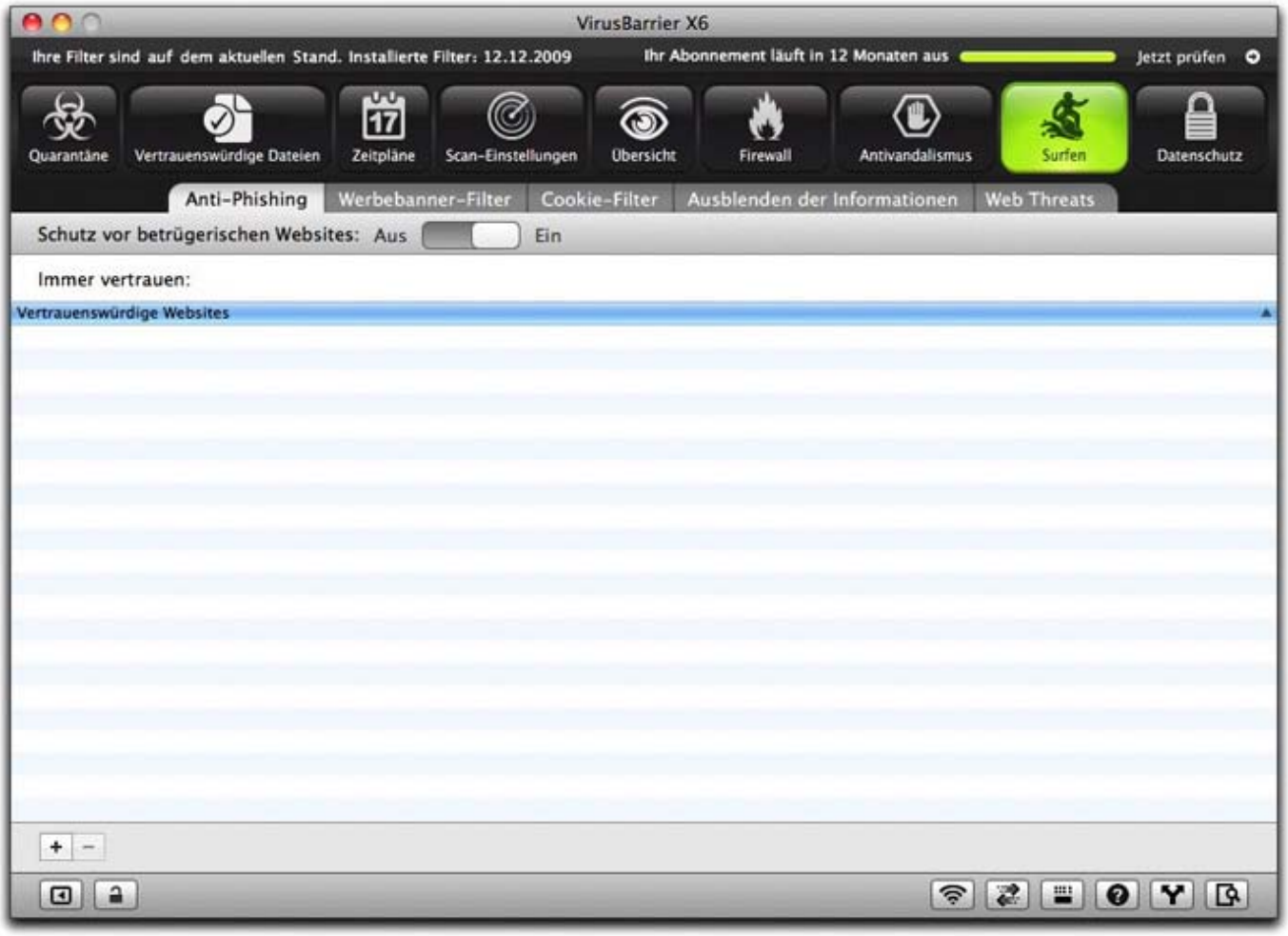
Surffilter

VirusBarrier X6 bietet Schutz vor Phishing-Web-Threats (Gefahren, die von Webseiten ausgehen, die "versteckte Munition" enthalten) und bietet drei Filter, mit denen Sie die Informationen kontrollieren können, die Ihr Mac sendet und empfängt, während Sie im Internet surfen.

Klicken Sie auf die Schaltfläche "Surfen", um sich die Surf-Einstellungen von VirusBarrier X6 anzeigen zu lassen.

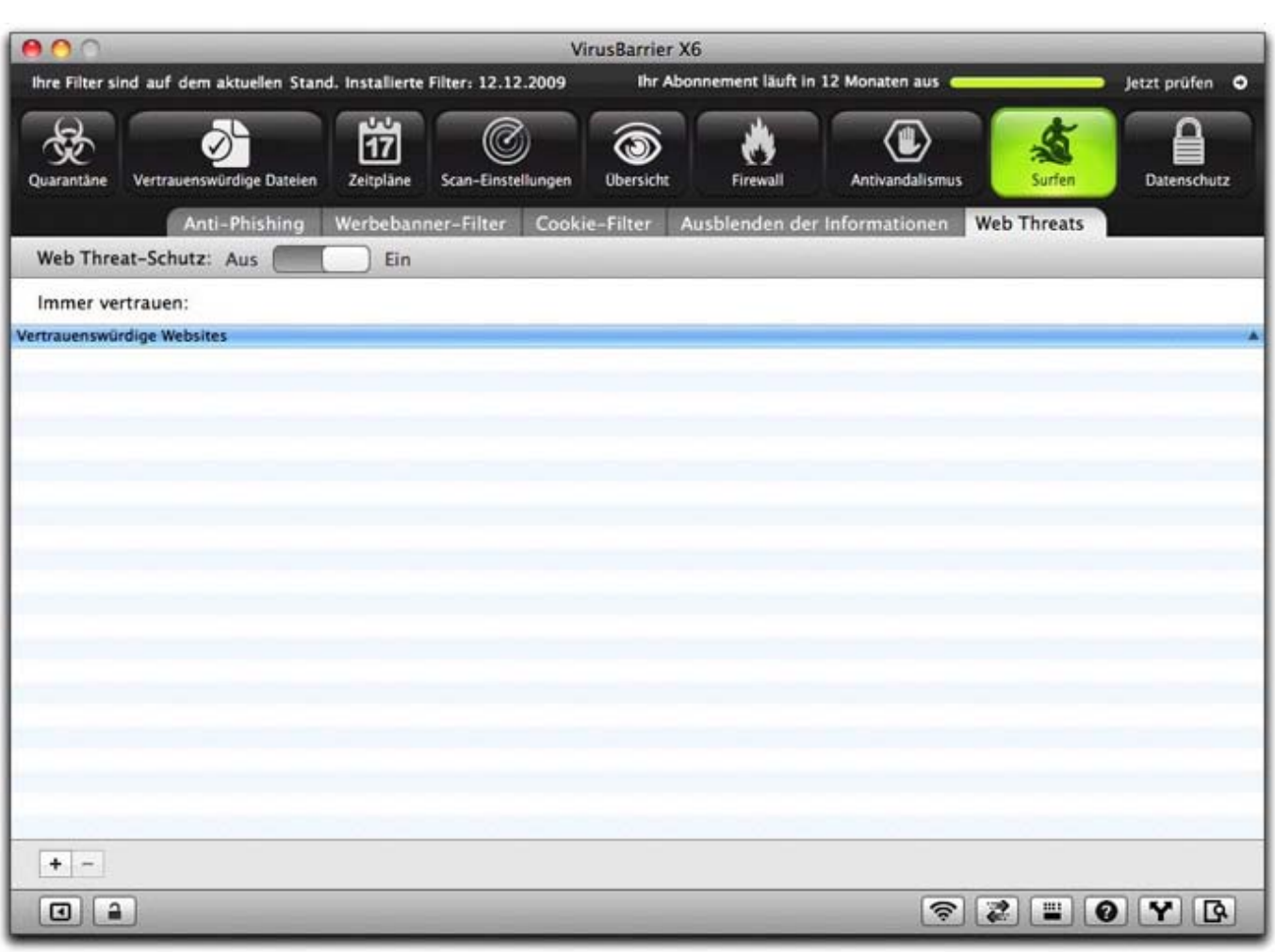
Der Anti-Phishing-Schutz von VirusBarrier X6 schützt Sie vor Phishing (Versuche Sie auszutricksen und dazu zu

bringen, persönliche Informationen auf betrügerischen Websites einzugeben, die echte Seiten imitieren). VirusBarrier X6 sperrt solche Seiten und schützt Sie so vor dieser Art von Betrug. Dennoch sollten Sie niemals auf einen Link in einer unverlangt empfangenen E-Mail klicken, wenn Sie deren Vertrauenswürdigkeit anzweifeln.



Schieben Sie zur Aktivierung des Anti-Phishing-Schutzes von VirusBarrier X6 den Schieberegler für den Schutz vor betrügerischen Websites auf "Ein". Sie können manuell Seiten hinzufügen, denen Sie immer vertrauen, indem Sie auf das Pluszeichen (+) unten im Fenster klicken und dann die URL der Seite eingeben, der Sie vertrauen. Sie sollten dies aber nur dann tun, wenn bestimmte Seiten unrichtigerweise als Phishing-Seiten markiert wurden.

VirusBarrier X6 bietet Schutz vor Web Threats, wie z.B. Cross-Site-Scripting-Angriffen (XSS), Heimliches Herunterladen von Software, Clickjacking sowie vor Webseiten mit schädlichem JavaScript oder schädlichen Java-Applets.



Schieben Sie zur Aktivierung des Web Threat-Schutzes von VirusBarrier X6 den Schieberegler für den Web Threat-Schutz auf "Ein". Sie können manuell Seiten hinzufügen, denen Sie immer vertrauen, indem Sie auf das Pluszeichen (+) unten im Fenster klicken und dann die URL der Seite eingeben, der Sie vertrauen. Sie sollten dies aber nur dann tun, wenn bestimmte Seiten unrichtigerweise als betrügerisch markiert wurden.

Drei weitere Surffilter helfen Ihnen bei der Auswahl, welche Art von Informationen Sie über Ihren Mac an Webserver senden möchten und unterstützen Sie dabei, werbefrei zu surfen:

- Die **Werbebanner-Filter** blenden Werbebanner auf den von Ihnen besuchten Websites aus.
- Der **Cookie-Filter** schützt Ihren Mac vor dem Senden bestimmter Informationen an Websites, die Ihr Verhalten beobachten.
- Der Filter zum **Ausblenden der Informationen** verhüllt bestimmte Informationen über Ihren Mac, den Webbrowser und die zuletzt von Ihnen besuchte Website.

Surffilter betreffen alle Computerprogramme, die über das HTTP-Protokoll kommunizieren. Webbrowser sind die bekanntesten Programme, die HTTP verwenden. Es ist jedoch ebenso Teil von iTunes, RSS-Newsreadern und vielen anderen Softwareprogrammen, die über die Fähigkeit zum Internetbrowsen verfügen. Wenn Sie unerwartete Schwierigkeiten mit solchen Programmen haben – beispielsweise beim Herunterladen von Musik über iTunes –, versuchen Sie die Surffilter vorübergehend zu deaktivieren.

Werbebanner-Filter

Der Werbebanner-Filter ist eine Liste von Regeln, die VirusBarrier X6 verwendet, um unerwünschtes Internetmaterial zu filtern, wie beispielsweise grafische Werbung ("Werbebanner"). So wird das Surfen wesentlich schnell und ungestörter. Werbebanner werden von VirusBarrier X6 gesperrt und durch kleine, transparente Grafiken ersetzt. VirusBarrier X6

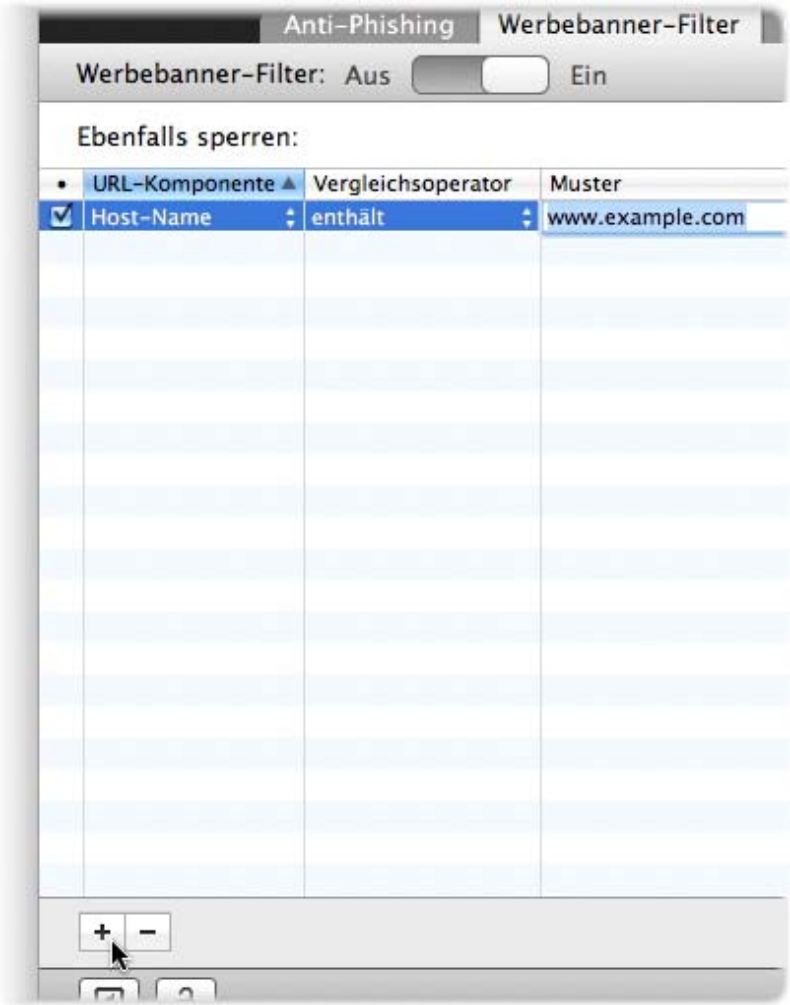
enthält eine interne Liste mit Werbebanner-Zeichenketten, die gefiltert werden. Sie können jedoch auch eigene Zeichenketten hinzufügen, damit noch mehr Werbung gefiltert wird, auf die Sie beim Surfen treffen.

Klicken Sie auf die Registerkarte "Werbebanner-Filter", damit Ihnen das Filter-Fenster angezeigt wird. Hier eine Abbildung mit einigen Beispieldaten:

Schieben Sie zur Aktivierung des Werbebanner-Filters den Schieberegler "Werbebanner-Filter" auf "Ein".

So fügen Sie Regeln für den Werbebanner-Filter hinzu

Der Werbebanner-Filter enthält bereits eine Reihe von Regeln, die jedes Mal aktualisiert werden, wenn Sie Ihre Filter für VirusBarrier X6 aktualisieren. Sie können jedoch auch einfach Ihre eigenen Regeln hinzufügen. Klicken Sie auf die Schaltfläche +, um dem Werbebanner-Filter Regeln hinzuzufügen. So wird der Werbebanner-Liste eine neue Zeile hinzugefügt, die Sie bearbeiten können.



Die Liste besteht aus vier Spalten: ein Kontrollkästchen, URL-Komponente, Vergleichsoperator und Struktur. Die Struktur bezeichnet offenkundig, wie Sie festlegen, was gesperrt werden soll.

Das Popup-Menü für die URL-Komponente bietet drei Optionen. VirusBarrier X6 sucht jeden Werbebanner-Filter in dem ausgewählten Element:

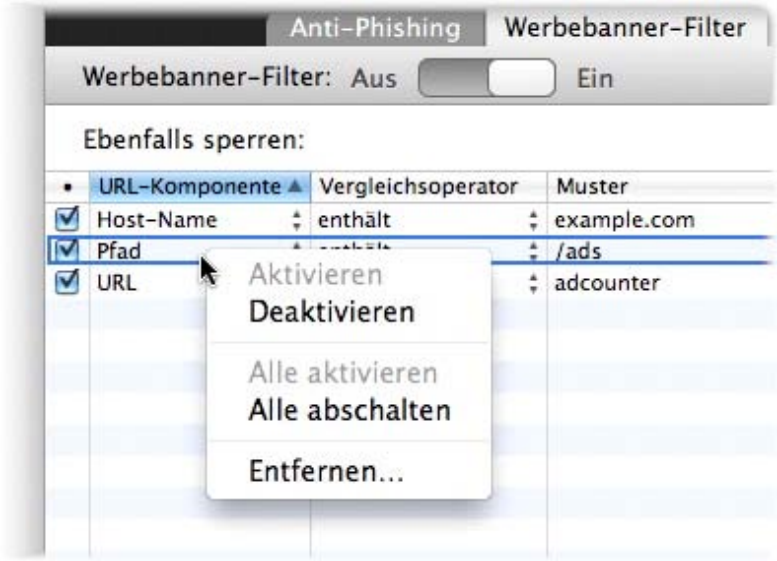
- **Host-Name**: Die Internetdomäne - also alles in einer Webadresse zwischen "http://" und dem ersten "/". Der Standardwert lautet "www.beispiel.com". Beachten Sie bitte, dass ein solcher Eintrag wie "http://foren.beispiel.com" dann (zum Beispiel) nicht gesperrt würde. Wenn Sie beides sperren möchten, sollten Sie einfach "beispiel.com" eingeben.
- **Pfad**: Jeder Teil der URL, der auf den Hostnamen folgt, wie z.B. /ads/ in http://www.beispiel.com/home/graphics/ads/6542.html.
- **URL**: Die gesamte URL, wie z.B. http://www.beispiel.com/home/graphics/ads/6542.html.

Im Popup-Menü **Vergleichsoperator** können Sie wählen, ob Inhalte auf Grund einer genauen Übereinstimmung ("ist") gesperrt werden sollen oder wenn Ihr Text mindestens mit einem Teil der URL übereinstimmt ("enthält").

So aktivieren oder deaktivieren Sie Regeln für den Werbebanner-Filter

Jede Werbebanner-Regel wird im Fenster für Werbebanner in einer eigenen Zeile angezeigt. Mit Hilfe des Kontrollkästchens links von jeder Zeile können Sie den Filter für jede Bannerregel aktivieren oder abschalten. Wenn Sie eine neue Bannerregel hinzufügen, wird das Kontrollkästchen automatisch markiert, wodurch angezeigt wird, dass der Filter für diese Regel aktiviert wurde. Wenn Sie das Sperren bestimmter Banner stoppen möchten, entfernen Sie die Häkchen aus den Kontrollkästchen für die entsprechenden Werbebanner.

Sie können auch das Sperren von Bannern für eine bestimmte Bannerregel oder für alle Bannerregeln aktivieren. Klicken Sie hierzu bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf den Namen einer Bannerregel. Nun wird ein Kontextmenü geöffnet.



Wählen Sie die Menüoption "Abschalten" für die gewünschte Bannerregel oder die Menüoption "Alle abschalten", um den Schutz für alle Bannerregeln zu deaktivieren. (Wenn die Regel bereits deaktiviert war, werden die Optionen "Aktivieren" und "Alle aktivieren" eingeblendet).

Wählen Sie zum Entfernen von Bannerregeln entweder die Option "Entfernen" aus dem Kontextmenü oder klicken Sie auf die Schaltfläche - unterhalb der Liste mit Werbebanner-Regeln.

Beachten Sie bitte, dass der Bannerfilter die Inhalte nicht erkennt, die gefiltert werden, sondern nur, ob die URL mit den Kriterien übereinstimmt, die Sie festgelegt haben. Sie werden daher möglicherweise in seltenen Fällen Schwierigkeiten haben, Informationen auf einer Webseite zu sehen, die zufälligerweise mit Ihren Kriterien übereinstimmen, tatsächlich aber keine Werbebanner sind. In diesem Fall versuchen Sie, den Bannerfilter vorübergehend auszuschalten. Sie können dies aus dem Programm VirusBarrier X6 heraus machen oder über das Intego-Menü in Ihrer Menüleiste.

Cookie-Filter

VirusBarrier X6 enthält einen Cookie-Filter, der dafür sorgt, dass Ihr Mac keine Verfolgungsinformationen, so genannte "Cookies", an Internetseiten sendet, außer an die von Ihnen angegebenen.

Der Cookiefilter ist hilfreich, wenn Sie absolut privat surfen möchten und nur einige wenige vertrauenswürdige Seiten über Ihre Aktivitäten informieren möchten. Viele Websites - vor allem solche, für die Sie ein Passwort benötigen - funktionieren jedoch nicht richtig, wenn Sie sie nicht ausdrücklich in die Liste vertrauenswürdiger Seiten aufnehmen.

Klicken Sie zum Einschalten des Cookie-Filters auf die Registerkarte "Cookie-Filter" und schieben Sie den Schieberegler "Cookie-Filter" auf "Ein".

Ihnen wird dann ein Hinweis angezeigt, dass bestimmte Seiten nicht richtig funktionieren werden, bis Sie diese der Liste mit vertrauenswürdigen Seiten hinzufügen. Klicken Sie zum Fortfahren auf "OK".

Wenn Sie diese Option aktivieren, können Sie eventuell nicht auf Websites zugreifen, für die Cookies aktiviert sein müssen.
Beispielsweise könnte der Zugriff auf Ihre Konten auf Seiten wie Facebook, YouTube oder Amazon verweigert werden, wenn diese Seiten sich nicht auf der Liste „Vertrauenswürdige Websites“ befinden.
OK

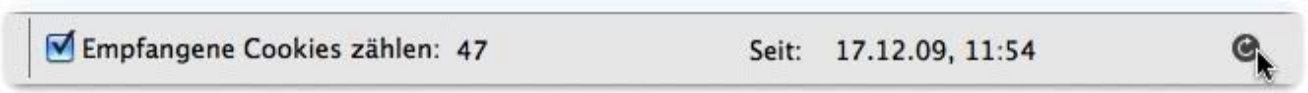
Wenn Sie der Cookie-Filterliste einen Server hinzufügen möchten, klicken Sie auf die Schaltfläche "+" am unteren Rand der Liste. Daraufhin wird eine Muster-Serveradresse (www.beispiel.com) angezeigt: Geben Sie anstelle dieser Adresse die Seite Ihrer Wahl ein.

Löschen Sie die Muster-Serveradresse und geben Sie den Namen des Servers ein, dem Sie es gestatten möchten, Ihnen Cookies zuzusenden. Sie können auch eine URL aus einem Browser oder sogar eine URL im Textformat in dieses Feld ziehen, um die Adresse der Liste hinzuzufügen.

Genau wie bei den Werbebanner-Filtern können Sie einzelne Server aktivieren oder deaktivieren. Klicken Sie hierzu jeweils auf das Kontrollkästchen daneben oder halten Sie die Steuerungstaste gedrückt, während Sie darauf klicken und verwenden Sie dann das Kontextmenü. Oder klicken Sie mit Ihrer rechten Maustaste darauf.

Cookie-Zähler

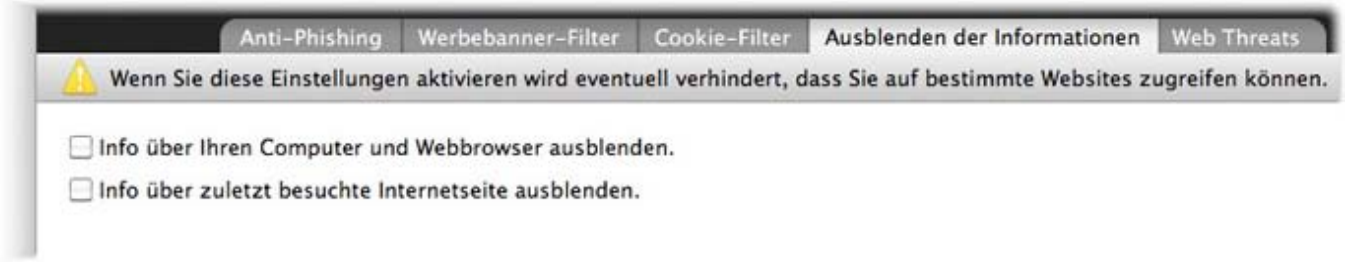
VirusBarrier X6 kann auch die Anzahl der an Ihren Mac gesendeten Cookies zählen. Hierzu müssen Sie nur das Kontrollkästchen **Empfangene Cookies zählen** am unteren Rand des Cookie-Filterfensters markieren. Ihnen wird dann angezeigt, wie viele Cookies Ihr Mac akzeptiert hat, seitdem Sie VirusBarrier X6 installiert haben oder seitdem Sie das letzte Mal den Zähler zurückgesetzt haben. Sie können den Zähler jederzeit auf Null zurücksetzen, indem Sie rechts auf den kleinen Pfeil klicken.



Ausblenden der Informationen

Alle Webbrowser reagieren auf Anfragen von Websites, mit denen festgestellt werden soll, welches Betriebssystem (Macintosh, Windows, Linux usw.) und welchen Webbrowser und welche Version Sie verwenden. Diese Information kann dazu beitragen, dass eine Seite Informationen auf die beste Weise verbreiten kann. So können beispielsweise nur die Funktionen eingeschaltet werden, die mit dem Webbrowser funktionieren, den Sie verwenden. Andererseits beschränken einige Seiten den Zugriff aber auch auf bestimmte Plattformen und Browser. Manchmal wird der Zugriff für alle verboten, die einen Mac verwenden. VirusBarrier X6 kann einige Informationen über Ihren Computer verbergen. So können Sie Zugriff auf Seiten erhalten, die Sie andernfalls nicht ansehen könnten.

Klicken Sie auf die Registerkarte "Ausblenden der Informationen", um die Einstellungen für das Ausblenden der Informationen anzusehen und zu ändern.


Anti-Phishing
Werbebanner-Filter
Cookie-Filter
Ausblenden der Informationen
Web Threats
Wenn Sie diese Einstellungen aktivieren wird eventuell verhindert, dass Sie auf bestimmte Websites zugreifen können.
Info über Ihren Computer und Webbrowser ausblenden.
Info über zuletzt besuchte Internetseite ausblenden.

Markieren Sie das Kontrollkästchen **Info über Ihren Computer und Webbrowser ausblenden**, um auf solche Anfragen von Websites nur durch das Senden allgemeiner Informationen zu antworten. So kann Ihr Computer beispielsweise einer Website antworten, dass Sie einen Mozillabrowser verwenden, aber ohne Versionsnummer oder Plattform.

Einige Websites beobachten auch, welche HTML-Seite Sie zuletzt geladen haben. Auch dies kann wiederum das Surfen im Web für Sie verbessern. Eine Einkaufsseite unterbreitet Ihnen beispielsweise bestimmte Angebote, wenn Sie von einer bestimmten Website kommen. Hemmungslose Betreiber bestimmter Seiten können diese Funktion jedoch auch verwenden, um Ihre Browseraktivitäten in einer Weise zu verfolgen, die Sie nicht möchten. Wenn Sie das Kontrollkästchen **Info über zuletzt besuchte Internetseite ausblenden** markieren, sorgt VirusBarrier X6 dafür, dass Ihr Mac auf diese Art von Anfragen nicht antwortet.

Schutz persönlicher Daten

Die Funktionen zum Datenschutz von VirusBarrier X6 untersuchen ein- und ausgehende Datenpakete, wobei sie nach bestimmten Datentypen suchen und so Ihre persönlichen Daten schützen. Klicken Sie auf die Schaltfläche "Datenschutz", um die Einstellungen für den Datenschutz anzusehen und zu ändern.

Anti-Spyware

Mit VirusBarrier X6 können Sie den Zugriff einzelner Programme von Ihrem Mac auf das Internet und auf lokale Netzwerke kontrollieren. Während Ihre Firewall-Einstellungen den allgemeinen Zugriff auf Netzwerke erlauben können, ermöglichen es Ihnen die Optionen auf der Registerkarte "Anti-Spyware", festzulegen, wie VirusBarrier X6 reagieren soll, wenn bestimmte Anwendungsprogramme versuchen, auf ein Netzwerk zuzugreifen. Dies ermöglicht Ihnen zwei Dinge:

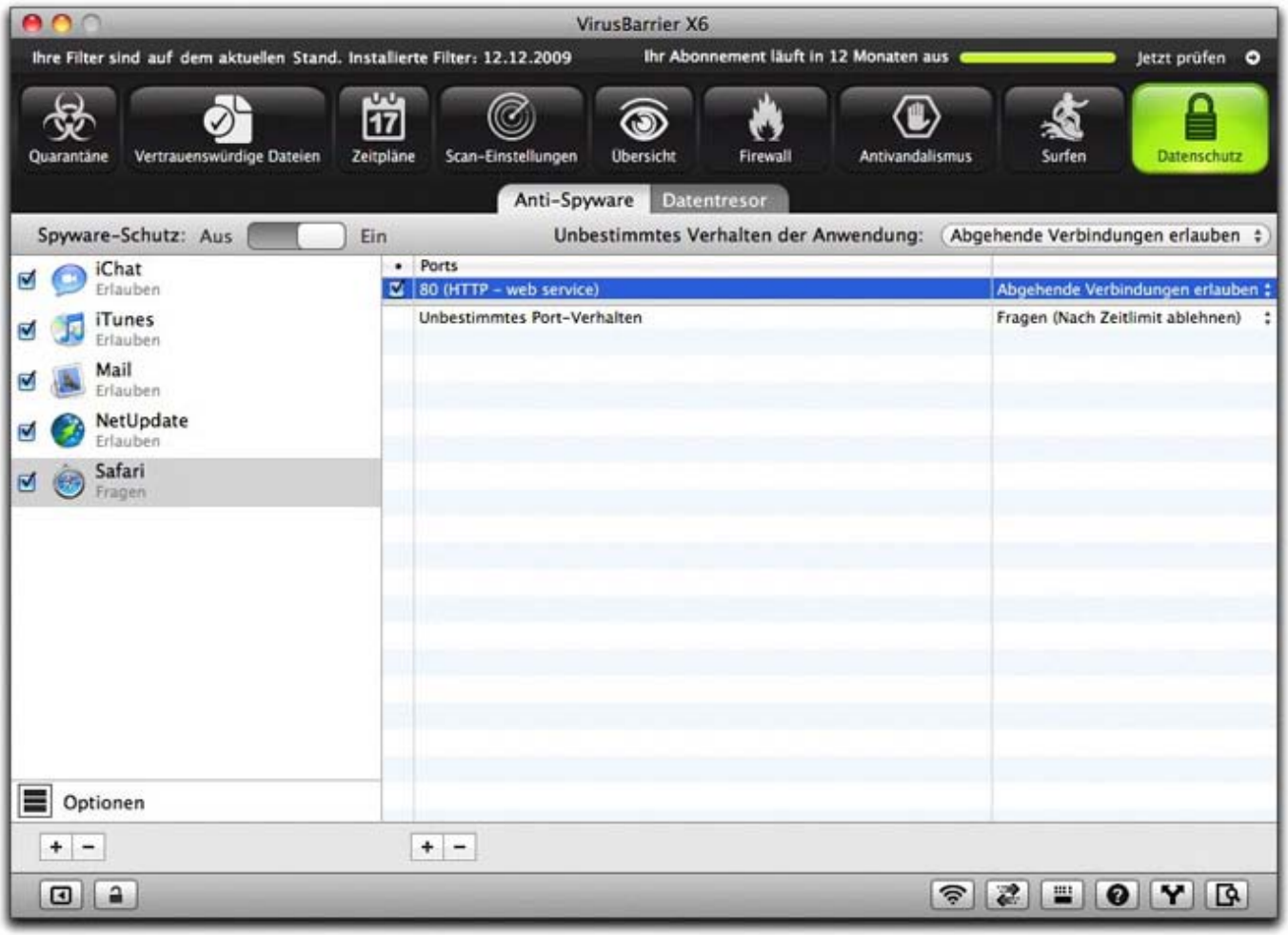
- Sie können verhindern, dass Benutzer mit bestimmten Programmen auf das Netzwerk zugreifen.
- Wenn ein Anwendungsprogramm versucht, hinter Ihrem Rücken eine Verbindung mit einem Netzwerk herzustellen, blockiert VirusBarrier X6 diesen Versuch, gibt eine Warnmeldung aus und fordert Sie auf, diesen Zugriff zu erlauben oder abzulehnen.

Auf Ihrem Mac gibt es viele Programme, die auf das Internet oder auf andere Netzwerke zugreifen. Hierzu zählen Webbrowser, E-Mail-Programme, FTP-Programme und Sofortnachrichtenprogramme (Instant Messaging). Vielleicht gibt es aber auch Programme, die eine Netzwerkverbindung herstellen, ohne Sie darüber zu informieren, um beispielsweise die Seriennummer eines auf Ihrem Computer installierten Anwendungsprogramms zu versenden, persönliche Daten über Sie zu sammeln und heimlich auf einen Server hochzuladen, oder eine Hintertür auf Ihrem Mac

zu öffnen, sodass Hacker oder Vandalen Zugriff auf Ihren Computer erhalten. VirusBarrier X6 benachrichtigt Sie über solche Versuche und gibt Ihnen die Möglichkeit zu entscheiden, ob Sie diese Versuche erlauben möchten.

Schieben Sie zum Einschalten der Anti-Spyware-Funktion den Schieberegler für den Spyware-Schutz auf "Ein".

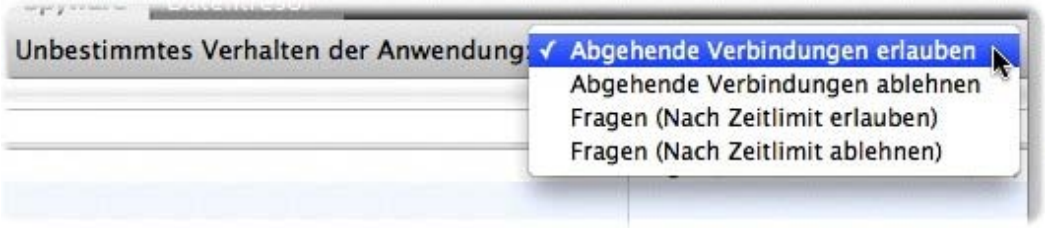
Anti-Spyware funktioniert folgendermaßen: Zuerst werden Sie gebeten, eine Liste mit Programmen zu erstellen, auf die diese Einstellungen angewendet werden sollen. Diese werden als "definierte" Programme bezeichnet, während alle Programme, die nicht auf der Liste stehen, als "undefiniert" gelten. Im obigen Beispiel ist Safari definiert, während der Webbrowser Firefox (der nicht auf der Liste steht) undefiniert ist.



Sobald Sie diese Liste erstellt haben, können Sie die Datenübertragung der definierten Programme genauer einstellen sowie eine allgemeine Richtlinie für undefinierte Programme einrichten. Zwei typische Konfigurationen wären beispielsweise folgende:

- Sie leiten ein Computerlabor und möchten, dass die Leute E-Mails mit dem Programm Mail von Apple versenden können. Sie sollen aber nicht im Internet surfen oder Netzwerkspiele spielen können. Sie würden also Mail als "Erlaubt" definieren, aber alle ausgehenden Verbindungen anderer Programme verbieten.
- Sie vermuten, dass ein Programm, das Sie auf Ihren Mac heruntergeladen haben, unautorisiert Daten versendet - vielleicht aus einer heimlich in das Programm eingebauten Spyware. Sie definieren dieses Programm und lehnen alle Datenübertragungen aus diesem Programm ab. Datenübertragungen aus undefinierten Programmen hingegen erlauben Sie.

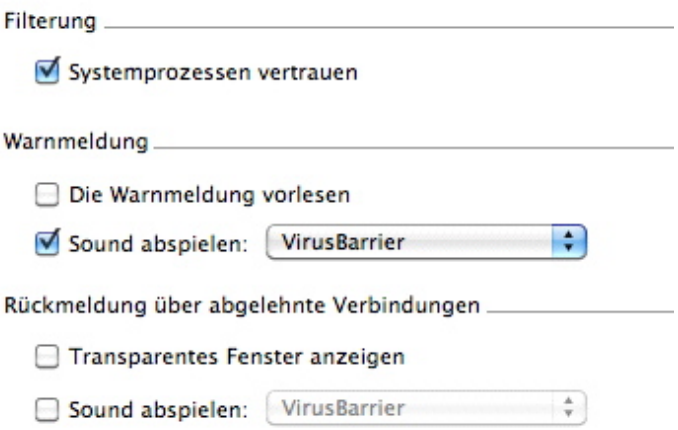
Für undefinierte Programme gibt es vier Verhaltensoptionen:



- **Abgehende Verbindungen erlauben**: VirusBarrier X6 erlaubt allen Anwendungsprogrammen den Zugriff auf das Internet und auf andere Netzwerke. Von Ihnen definierte Firewall-Regeln, womit Sie den Zugriff auf bestimmte Ports erlaubt oder gesperrt haben, bleiben jedoch in Kraft. Wenn beispielsweise ein FTP-Programm versucht, eine Verbindung mit einem Server herzustellen, wird der Internet-Zugriff durch dieses Anwendungsprogramm nicht von VirusBarrier X6 gesperrt. Wenn Sie aber eine Firewall-Regel definiert haben, durch die der Zugriff auf den Port 20 (den standardmäßigen FTP-Port) gesperrt wird, so wird die Datenübertragung blockiert. Wenn das FTP-Programm versucht, eine Verbindung über einen anderen Port herzustellen, wird es nicht blockiert.
- **Abgehende Verbindungen ablehnen**: VirusBarrier X6 sperrt jeden Zugriff auf das Internet und auf andere Netzwerke. Hierdurch werden alle von Ihnen definierten Firewall-Regeln außer Kraft gesetzt.
- **Fragen (Nach Zeitlimit erlauben)**: VirusBarrier X6 fragt Sie bei jedem Versuch eines Anwendungsprogramms, eine Verbindung herzustellen, ob Sie dies erlauben oder ablehnen wollen. Wenn Sie nicht innerhalb von 90 Sekunden antworten, wird dem Anwendungsprogramm der Zugriff auf das Internet für dieses eine Mal gestattet.
- **Fragen (Nach Zeitlimit ablehnen)**: VirusBarrier X6 fragt Sie bei jedem Versuch eines Anwendungsprogramms, eine Verbindung herzustellen, ob Sie dies erlauben oder ablehnen wollen. Wenn Sie nicht innerhalb von 90 Sekunden antworten, wird dem Anwendungsprogramm der Zugriff auf das Internet für dieses eine Mal nicht gestattet.

Optionen

Mit der Schaltfläche "Optionen" in der unteren linken Ecke des Fensterabschnitts "Anti-Spyware" können Sie einige allgemeine Einstellungen für die Anti-Spyware-Funktion konfigurieren.



Es gibt eine besondere Option für die Anti-Spyware-Funktion: "Systemprozessen vertrauen". Diese Option lässt Datenübertragungen der vielen Teile von Mac OS X selbst zu, die eine Internet- oder Netzwerkverbindung herstellen möchten. Hierzu zählen beispielsweise Druckerdienste, die Auflösung von Domänennamen, die Suche nach Software-Aktualisierungen oder die Synchronisation der Uhrzeit. Dabei handelt es sich um Anfragen von Teilen von Mac OS X, nicht um separate Programme. Wenn Sie diesen Prozessen vertrauen und nicht jedes Mal gefragt werden wollen, wenn diese eine Verbindung mit dem Internet oder dem lokalen Netzwerk herstellen wollen, müssen Sie das Kontrollkästchen "Systemprozessen vertrauen" markieren.

Die anderen Optionen beziehen sich auf Warnmeldungen und Rückmeldungen, wenn Verbindungen gesperrt wurden. Wählen Sie die Optionen entsprechend der Art aus, auf die Sie bei nicht autorisierten oder gesperrten Verbindungen gewarnt werden möchten. Weitere Informationen über diese Optionen erhalten Sie unter "Die Bedeutung von Warnmeldungen" weiter hinten in diesem Benutzerhandbuch.

Programme: Hinzufügen, Entfernen und Ändern von Einstellungen

Nachdem Sie ausgewählt haben, ob der Netzwerkzugriff von undefinierten Programme erlaubt oder abgelehnt werden soll, können Sie ein Programm definieren. Klicken Sie hierzu auf das Pluszeichen, navigieren Sie dann durch das Dialogfeld von Mac OS X bis zum Programm selbst und fügen Sie es hinzu. (Sie können Programme auch hinzufügen, indem Sie deren Symbole aus dem Finder ziehen.) Wiederholen Sie diesen Vorgang für alle Programme, die Sie hinzufügen möchten. (Wenn Sie ein Programm aus der Liste löschen möchten, klicken Sie darauf und klicken Sie dann auf das Minuszeichen am unteren Rand der Programmliste).

Sie können die Einstellungen dann für jedes Programm ändern, um Datenübertragungen von dem Programm vollständig oder über bestimmte Ports zu erlauben oder abzulehnen. Ähnlich wie bei dem vorigen Vorgang, als Sie festgelegt haben, was passieren soll, wenn undefinierte Programme versuchen, Daten zu versenden, können Sie jetzt festlegen, was passieren soll, wenn ein bestimmtes Programm eine Datenübertragung von einem undefinierten Port versucht. Dann definieren Sie eine Liste mit Ports für dieses bestimmte Programm, die eine Ausnahme für die allgemeine Regel bilden.

Im obigen Beispiel:

- Fünf Programme (auf der linken Seite aufgeführt) haben bestimmte Regeln, durch die sie verwaltet werden. Ausgehende Verbindungen sind von allen anderen Programmen erlaubt.
- Firefox darf zwei Arten der Datenübertragung senden, über die Ports 80 und 8080.
- Datenübertragungen von Firefox über Port 443 sind verboten.
- Bei Datenübertragungen von Firefox über jeden anderen Port wird auf dem Bildschirm Ihres Mac eine Warnmeldung angezeigt. Wenn Sie die Datenübertragung nicht innerhalb von 90 Sekunden erlauben, wird diese verboten.

Diese Portliste besteht aus drei Spalten:

- In der ersten Spalte, die mehrere Kontrollkästchen enthält, wird das für das Programm derzeit aktivierte Portverhalten angezeigt. Wenn das Kästchen neben einem Port markiert ist, wurde das von Ihnen festgelegte Verhalten aktiviert. Wenn Sie dieses Verhalten deaktivieren möchten, müssen Sie das Häkchen aus dem Kästchen entfernen. Sie können das Verhalten später erneut aktivieren, indem Sie das Kästchen wieder markieren.
- Die zweite Spalte mit der Überschrift "Ports" zeigt Ihnen Informationen über die Ports an, die das Programm für den Netzwerkzugriff verwendet. Hier erfahren Sie die Port-Nummer und manchmal auch das verwendete Protokoll sowie eine kurze Beschreibung. (Diese Beschreibung wird automatisch angezeigt, wenn Sie eine Portnummer eingeben, die VirusBarrier X6 erkennt). Sie können eine Port-Nummer oder eine Reihe von Port-Nummern hinzufügen, beispielsweise 110-123.

- Die dritte Spalte enthält entweder "Abgehende Verbindungen erlauben" oder "Abgehende Verbindungen ablehnen". Sie können jederzeit von einer Option zur anderen wechseln, indem Sie auf den Text klicken.

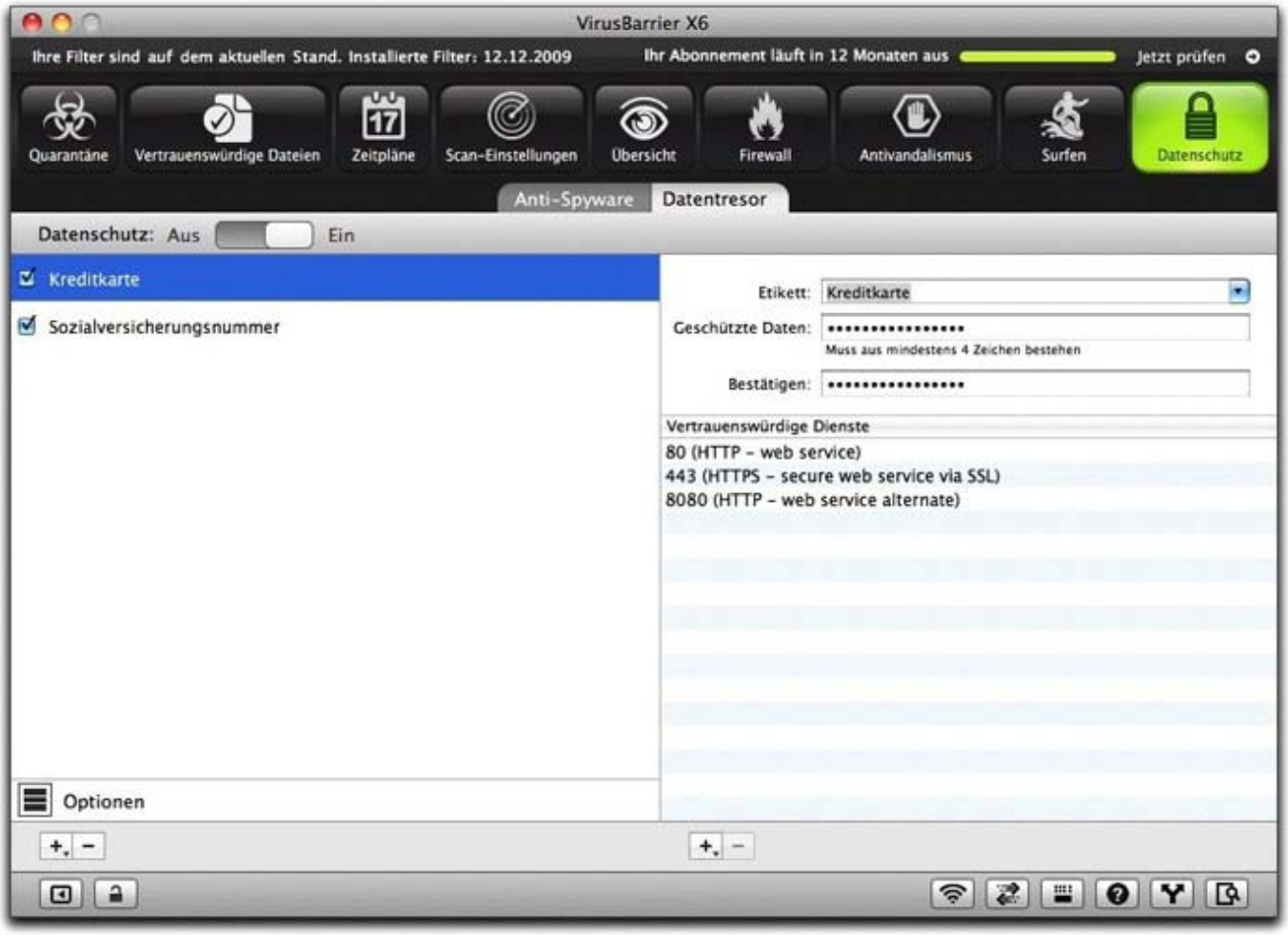
Wenn Sie sich ein Programm auf der Programmliste im Finder anzeigen lassen möchten, müssen Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf den Namen des entsprechenden Anwendungsprogramms klicken. Daraufhin wird ein Kontextmenü geöffnet. Wählen Sie die Menüoption "Im Finder anzeigen". Nun wird ein Fenster im Finder geöffnet, in dem Ihnen der Speicherort des Anwendungsprogramms auf Ihrem Computer angezeigt wird. So können Sie Programme leichter finden, die nach Warnmeldungen oder Zeitüberschreitungen hinzugefügt wurden.

Hinweis: Eine Möglichkeit die Anti-Spyware-Funktion von VirusBarrier X6 zu verwenden besteht darin, sie einzuschalten und das Programm nachfragen zu lassen, ob Programme sich mit dem Internet verbinden dürfen. Jedes Mal wenn das passiert (nur einmal pro Programm und Port) fügen Sie die Programme, die Sie zulassen möchten, hinzu und erweitern so langsam Ihre Liste. Auf diese Weise sehen Sie jedoch nur, wie viele Programme sich mit Remote-Servern verbinden. Bedenken Sie bitte, dass viele Programme diese Verbindungen nur nutzen, um nach Aktualisierungen zu suchen, da viele Programme über integrierte Aktualisierungsfunktionen verfügen.

Datentresor

Der Datentresor stellt sicher, dass sensible, auf Ihrem Mac gespeicherte Daten von diesem nicht über ein Netzwerk versendet werden können. Sie entscheiden selbst, welche Daten geschützt werden sollen: Ihre Kreditkartennummer, Passwörter oder Schlüsselwörter aus vertraulichen Dokumenten usw. Der in VirusBarrier X6 integrierte Datenfilter überprüft jedes ausgehende Datenpaket und stellt so sicher, dass keine Dokumente versendet werden, die diese Informationen enthalten. So werden Sie nicht nur vor dem versehentlichen Versenden von Dokumenten mit diesen Informationen geschützt. Das Programm sorgt auch dafür, dass niemand anderes mit einem Netzwerkzugang zu Ihrem Mac Kopien davon machen kann.

Klicken Sie auf die Schaltfläche "Datenschutz" und dann auf die Registerkarte "Datentresor", um den Fensterabschnitt "Datentresor" zu öffnen.



So funktioniert der Datentresor

VirusBarrier X6 prüft alle Datenpakete, die von Ihrem Computer in das Internet oder in ein lokales Netzwerk gesendet werden. Wenn irgendwelche der im Filter spezifizierten Daten gefunden werden, wird das Paket blockiert.

Der Datentresor blockiert nur die Daten, die *genau* mit dem angegebenen Text übereinstimmen, einschließlich der Satzzeichen und des Kasus. Wenn Sie beispielsweise Ihre Kreditkartennummer als zu schützende Daten angegeben haben, sorgt VirusBarrier X6 dafür, dass diese Daten Ihren Computer nicht verlassen und kann Sie auf verschiedene Weise warnen, wenn Sie diese Option wählen. Wenn Sie jedoch die gleiche Nummer auf einer sicheren Webseite eingeben, verschlüsselt Ihr Browser diese Nummer. Die Daten stimmen daher nicht mehr mit den zu schützenden Daten überein und werden gesendet. Das Gleiche gilt für auf andere Weise codierte oder komprimierte Daten.

In sehr seltenen Fällen sperrt der Datentresor Daten, die zwar mit Ihren Kriterien übereinstimmen, nicht jedoch mit Ihrer Absicht. Eine Grafikdatei (z.B. ein Bild auf einer Website) besteht im Wesentlichen aus einer Zeichenkette, die Tausende von Zeichen lang ist. Möglicherweise kann eine Grafikdatei einen Datenteil enthalten, den Sie schützen möchten. Daher würde dieser Teil dann durch den Datentresor gesperrt. (Wenn Sie beispielsweise den Namen "Jodie" blockieren möchten und eine Grafikdatei die Zeichenkette "Cg34gb$sEbOJodie8%" enthält, würde diese gesperrt. Wenn Sie feststellen, dass Sie einen bestimmten Informationsteil nicht senden oder empfangen können, schalten Sie den Datentresor vorübergehend aus und schalten Sie ihn dann wieder ein, wenn die Informationen übertragen wurden.

Schieben Sie den Schieberegler "Datenschutz" in der oberen linken Ecke auf "Ein", um den Datentresor zu aktivieren. Sie können diese Option jederzeit wieder deaktivieren. Beispielsweise wenn Sie vorübergehend erlauben möchten, dass Ihre geschützten Daten versendet werden. Sie können die Funktion auch über das Intego-Menü in Ihrer Menüleiste ausschalten.

Diese Daten können geschützt werden

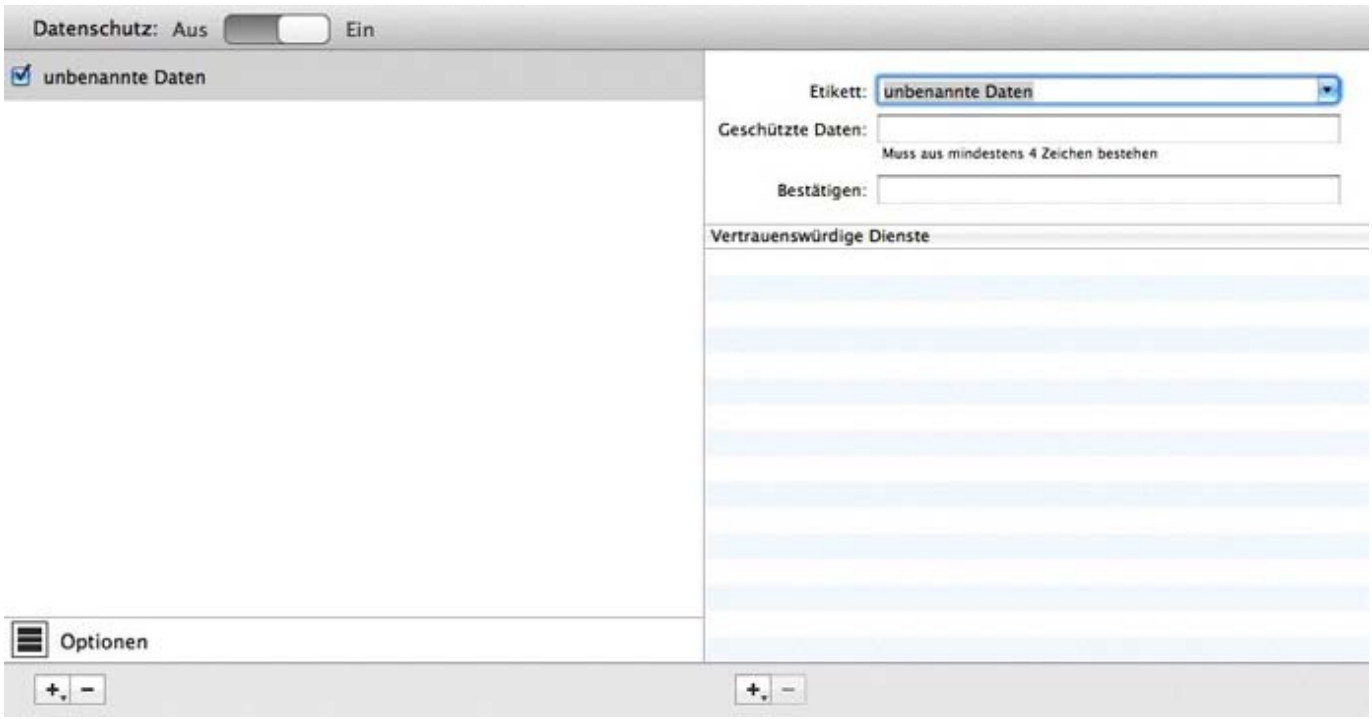
Der Datentresor enthält Etiketten für die sechs häufigsten Arten sensibler Informationen:

- **Kreditkarten**
- **E-Mail-Adressen**
- **Privatadressen**
- **Namen**
- **Sozialversicherungsnummern**
- **Telefonnummern**

Diese Etiketten dienen jedoch nur der einfachen Handhabung. VirusBarrier selbst behandelt diese Informationen nicht anders als andere oder anders als alle weiteren Informationsarten, die Sie eventuell später eingeben – beispielsweise "Telefonnummer", "Name des Kindes" oder "Passwörter".

So fügen Sie dem Tresor Daten hinzu

Wenn Sie dem Datentresor Daten hinzufügen möchten, klicken Sie auf die Schaltfläche + unter dem Symbol für Optionen. Daraufhin wird in der Filterliste ein neuer Eintrag mit der Bezeichnung "unbenannte Daten" angezeigt.

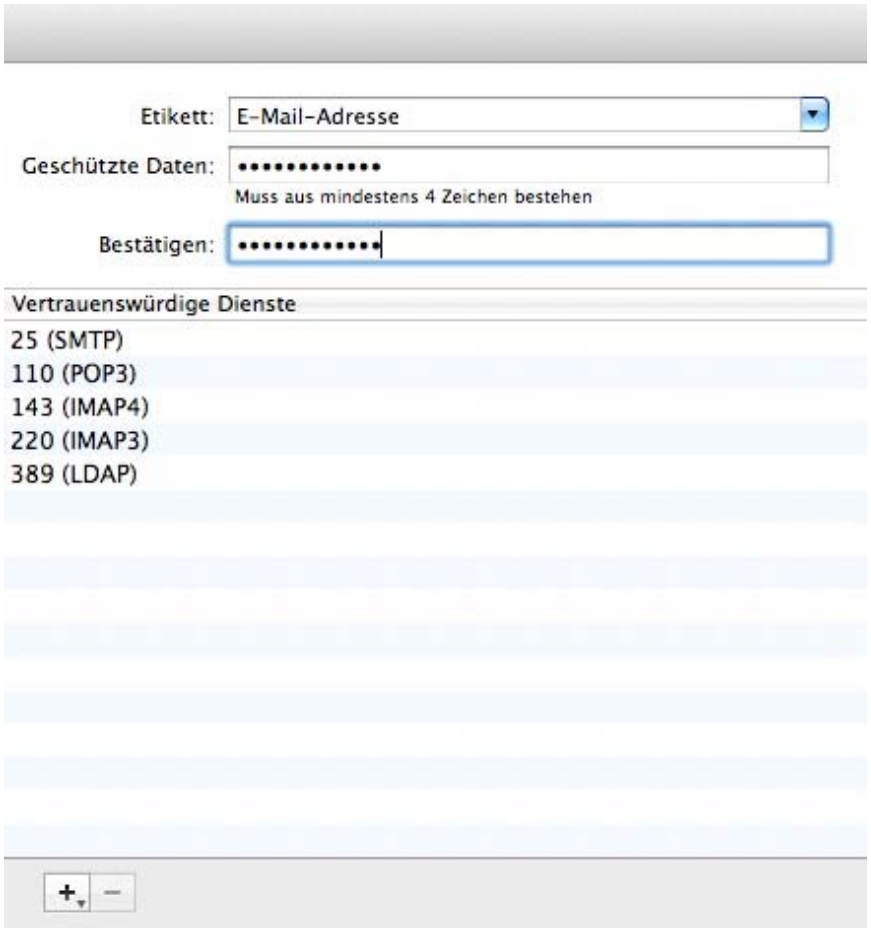


Geben Sie eine Beschreibung für Ihre geschützten Daten in das Bezeichnungsfeld ein oder wählen Sie diese aus dem Popup-Menü: Sie werden feststellen, dass diese Beschreibung in der Tresorliste wiedergegeben wird. Geben Sie dann die Daten, die tatsächlich geschützt werden sollen, in das Textfeld "Geschützte Daten" ein. Der Text wird ausgeblendet, so kann niemand sich diese Daten über Ihre Schulter ansehen oder sie bei einem späteren Zugriff auf Ihren Mac sehen. Die Daten müssen Sie dann noch einmal in das Bestätigungsfeld eingeben. Wenn die Eingabefelder für die zu schützenden Daten und die Bestätigung nicht übereinstimmen, wird ein Fenster eingeblendet, in dem Sie dann entweder die zu schützenden Daten noch einmal in beide Datenfelder eingeben oder auf die Schaltfläche "OK" klicken können. Wenn Sie auf "OK" klicken, müssen Sie nur das Bestätigungsfeld neu ausfüllen.

Sie müssen den Text *exakt* so eingeben, wie er in den entsprechenden Dokumenten enthalten ist. Beispielsweise kann eine Kreditkartennummer in einem Dokument im Format ####-####-####-#### oder #### #### #### #### enthalten sein. Wenn Sie Ihre Kreditkartennummer nur im ersten Format eingeben, kann der Filter Ihre

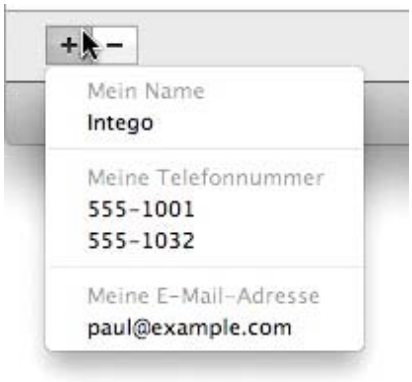
Kreditkartennummer nicht schützen, wenn sie in einem Dokument im zweiten Format enthalten ist. Achten Sie bei der Eingabe zu schützender Daten auch unbedingt auf korrekte Groß- und Kleinschreibung. Wenn Sie ein Schlüsselwort wie z.B. einen Projektnamen eingeben wollen, müssen Sie dies in allen möglichen Varianten tun: z.B. Marktuntersuchung, Markt-Untersuchung, MARKTUNTERSUCHUNG.

Im Abschnitt "Vertrauenswürdige Dienste" können Sie auswählen, dass Daten für alle bis auf die ausgewählten Diensten gesperrt werden sollen. Klicken Sie hierzu auf die Schaltfläche + unterhalb der Liste mit vertrauenswürdigen Diensten. Geben Sie anschließend die Port-Nummer des Dienstes ein. Alternativ können Sie auch auf das Pluszeichen (+) klicken und die Maustaste wenige Sekunden lang gedrückt halten: Sie können dann in einer Popup-Liste aus den am häufigsten gebrauchten Diensten wählen. (Einige davon, wie beispielsweise Mail im Beispiel unten, fügen mehrere Ports auf einmal hinzu.) Sie können eine Port-Nummer oder eine Reihe von Port-Nummern hinzufügen, beispielsweise 110-123. Daten zu diesem Port (oder diesen Ports) werden nicht gesperrt. Wenn Sie andere Dienste hinzufügen wollen, müssen Sie den vorstehend beschriebenen Vorgang wiederholen. Sie können beliebig viele Dienste hinzufügen.



Sie können Dienste auch per Drag&Drop aus der Dienste-Bibliothek hinzufügen. Dies ist besonders dann hilfreich, wenn Sie die entsprechenden Port-Nummern nicht kennen, die Sie der Liste hinzufügen möchten. Wählen Sie "Fenster > Dienste-Bibliothek" oder drücken Sie Wahltaste-Befehlstaste-6, um sich die Dienste-Bibliothek anzeigen zu lassen. Wählen Sie den gewünschten Dienst und ziehen Sie ihn auf die Liste mit vertrauenswürdigen Diensten.

Sie können bestimmte persönliche Informationen von Ihrer Karte im Adressbuch von Apple hinzufügen, wenn Sie ein Feld ausgefüllt haben. Klicken Sie hierzu auf die Schaltfläche + unterhalb der Datentresorliste in der linken Spalte und halten Sie diese gedrückt. Ihnen werden dann Elemente angezeigt, die in drei Gruppen aufgeteilt sind: Mein Name, Meine Telefonnummer und Meine E-Mail-Adresse. Wählen Sie eines der Elemente aus, um es zu den geschützten Daten hinzuzufügen.



Sobald Sie diese Informationen vollständig eingegeben haben, werden Ihre Daten geschützt. Sie können jederzeit zurückkehren, um das Datenelement zu bearbeiten. Klicken Sie hierzu in der Datentresorliste auf das Element und ändern Sie die Informationen in dem zugehörigen Fensterabschnitt auf der rechten Seite.

So aktivieren, deaktivieren und löschen Sie Datenelemente

Jedes geschützte Objekt wird im Datentresorfenster in einer eigenen Zeile angezeigt. Mit Hilfe des Kontrollkästchens links von jeder Zeile können Sie den Filter für das betreffende Objekt aktivieren oder abschalten. Wenn Sie ein neues Objekt hinzufügen, wird das Kontrollkästchen links davon automatisch markiert. So wird angezeigt, dass der Filter für dieses Objekt aktiviert wurde. Wenn Sie diese Daten über das Internet oder ein lokales Netzwerk versenden möchten, müssen Sie das Häkchen aus dem Kontrollkästchen für das entsprechende Element entfernen. Oder Sie deaktivieren alle Datentresore, indem Sie den Schieberegler für den Datenschutz wie zuvor beschrieben auf "Aus" stellen.

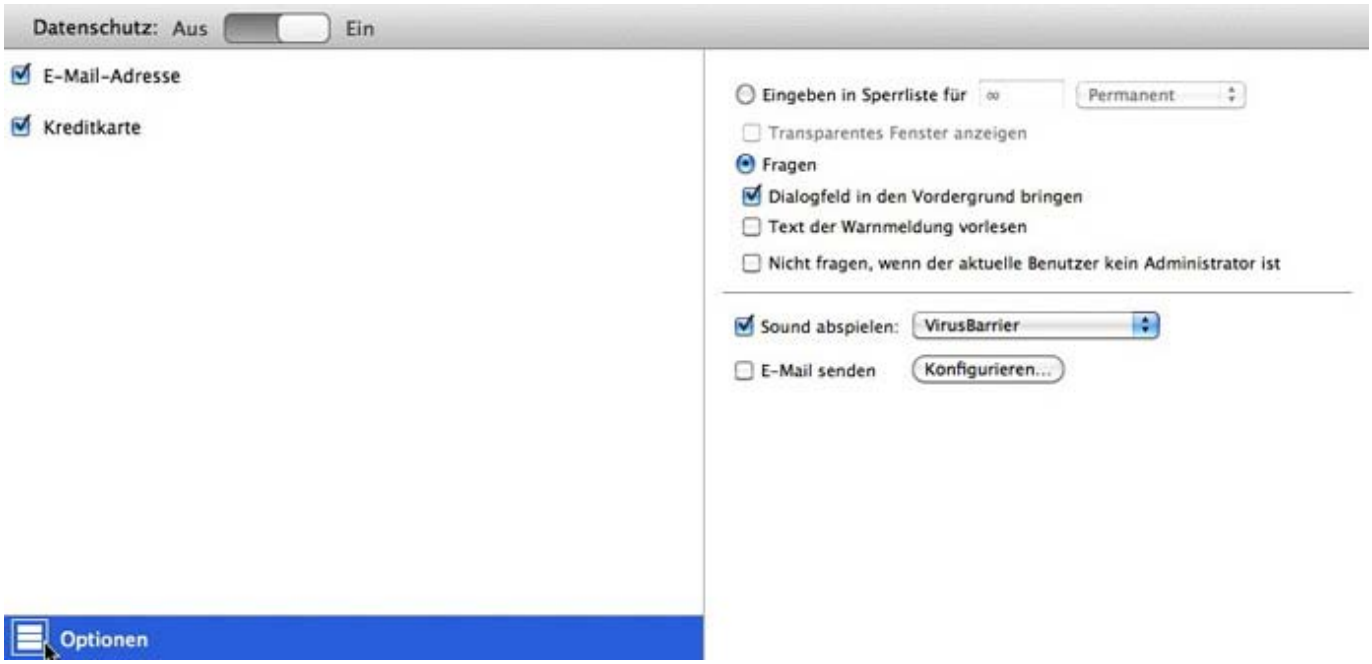
Sie können die Datenfilter für einzelne oder alle geschützten Daten aktivieren oder deaktivieren. Klicken Sie hierzu bei gedrückter Taste "ctrl" auf der Tastatur Ihres Macintosh auf den Namen eines Datenelements oder klicken Sie mit Ihrer rechten Maustaste. Daraufhin wird ein Kontextmenü geöffnet.

Wählen Sie die Menüoption "Abschalten" für das gewünschte Objekt oder die Menüoption "Alle abschalten", um den Schutz für alle Objekte zu deaktivieren. (Wenn das ausgewählte Element im obigen Beispiel bereits deaktiviert worden wäre, stünden die Optionen "Aktivieren" bzw. "Alle aktivieren" zur Verfügung.)

Wenn Sie das Element dauerhaft aus der Datentresorliste entfernen möchten, klicken Sie entweder auf die rechte Maustaste, wie zuvor beschrieben, und wählen Sie "Entfernen..." oder wählen Sie das Datenelement aus und klicken Sie dann auf die Schaltfläche -. In beiden Fällen werden Sie in einem Dialogfeld aufgefordert, das Löschen des Datenelements zu bestätigen.

Datentresor-Optionen

Wenn versucht wird, geschützte Daten von Ihrem Mac zu senden oder darauf zu empfangen, können Sie auf verschiedene Weise darüber informiert werden. Sie können auch wählen, was künftig in solchen Fällen getan werden soll. Klicken Sie auf die Schaltfläche "Optionen" in der unteren linken Ecke des Datenfensters, um sich diese Optionen anzeigen zu lassen. Änderungen an den Datentresor-Optionen haben Auswirkungen auf alle Datentresore.



Diese Optionen werden weiter im nächsten Abschnitt "Die Bedeutung von Warnmeldungen" erklärt.

Die Bedeutung von Warnmeldungen

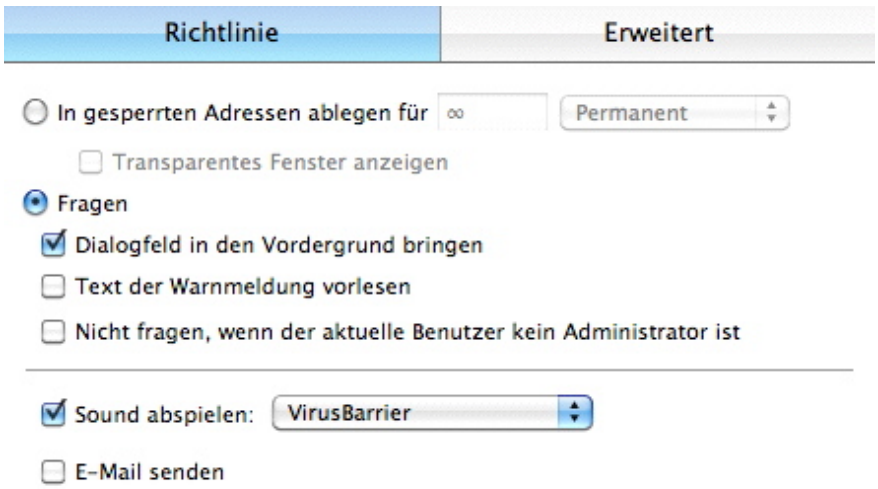
VirusBarrier X6 überwacht die Netzwerkaktivitäten Ihres Computers zum Internet und zu lokalen Netzwerken dauerhaft und sucht nach bestimmten Datentypen, die auf einen Eindringversuch oder einen Angriff hinweisen. Wenn verdächtige Datenpakete gefunden werden, gibt VirusBarrier X6 eine Warnmeldung aus, wobei Sie gleichzeitig gefragt werden, ob das Senden der Datenpakete zugelassen oder verweigert werden soll. Ebenso wie die Warnmeldungen bei schädlicher Software, die unter So schützen Sie Ihren Mac vor Viren und schädlicher Software erklärt werden, zeigt VirusBarrier X6 Warnmeldungen an, wenn bestimmte Netzwerkereignisse auftreten.

Einstellungen für die Warnmeldungen

Netzwerk-Warnmeldungen werden angezeigt, wenn eine Reihe von Netzwerkereignissen auftreten. Dazu zählt, wenn Trojanische Pferde entdeckt werden, wenn geschützte Daten von Ihrem Mac versendet werden, wenn die Anti-Spyware-Funktion entdeckt, dass ein undefiniertes Programm sich mit dem Internet zu verbinden versucht, wenn die Firewall Daten blockiert und mehr.

Einstellungen für diese Warnmeldungen tauchen an mehreren Stellen in VirusBarrier X6 auf, wie in den entsprechenden Abschnitten dieses Handbuchs beschrieben. Zur Erklärung dieser Einstellungen sehen wir uns an, wie sie im Abschnitt

für Antivandalismus-Richtlinien auftauchen.



- **In gesperrten Adressen ablegen**: Wenn dieses runde Optionsfeld markiert ist, wird die Verbindung bei der Ausgabe einer Warnmeldung automatisch unterbrochen. Die IP-Adresse des angreifenden Computers wird automatisch in die Liste mit gesperrten Adressen aufgenommen. In einem Feld rechts vom runden Optionsfeld können Sie angeben, wie lange die IP-Adresse standardmäßig in der Liste mit gesperrten Adressen gespeichert werden soll. Sie können diese Zeitdauer in Sekunden, Minuten, Stunden oder Tagen angeben oder festlegen, dass die IP-Adresse des angreifenden Computers dauerhaft in die Liste mit gesperrten Adressen aufgenommen werden soll. (Was passiert, wenn das Kontrollkästchen "Transparentes Fenster anzeigen" markiert ist, wird im nächsten Abschnitt "Beispiele für Warnmeldungen" gezeigt.)
- **Fragen**: Wenn dieses runde Optionsfeld markiert ist, zeigt VirusBarrier X6 einen Warndialog an, in dem Sie gefragt werden, was passieren soll. Wenn eine Warnmeldung erscheint, zeigt diese den standardmäßig gewählten Zeitraum der Liste mit gesperrten Adressen an. Dieser Zeitraum kann jedoch auf der Registerkarte für Richtlinien für jede Angriffsart geändert werden. Zudem haben Sie drei Optionen:
    - **Dialogfeld in den Vordergrund bringen**: Die Warnmeldung wird bei einem Alarm automatisch in den Vordergrund gebracht. Andernfalls bleiben diese Fenster im Hintergrund (also hinter eventuellen anderen Fenstern auf dem Bildschirm Ihres Computers). Wenn Sie 90 Sekunden lang nicht auf eine Warnmeldung reagieren, wird das Fenster automatisch geschlossen. Die betreffende Verbindung mit Ihrem Computer wird abgelehnt.
    - **Text der Warnmeldung vorlesen**: VirusBarrier X6 verwendet die Funktion "Text-to-Speech" von Mac OS X, um den Text der Warnmeldung vorzulesen.
    - **Nicht fragen, wenn der aktuelle Benutzer kein Administrator ist**: VirusBarrier X6 bietet die obigen Optionen nur an, wenn der Benutzer von Mac OS X über Administratorrechte verfügt. Andernfalls wird der angreifende Host automatisch in die Liste mit gesperrten Adressen aufgenommen.
- **Sound abspielen**: VirusBarrier X6 spielt bei jedem Alarm einen akustischen Warnhinweis Ihrer Wahl. Aus dem Popup-Menü rechts neben der Schaltfläche können Sie die gewünschte Klangdatei wählen. (Der Ton wird abgespielt, sobald Sie die Auswahl vorgenommen haben.)
- **E-Mail senden**: VirusBarrier X6 sendet automatisch innerhalb von 30 Sekunden eine E-Mail an die Adresse, die auf der Registerkarte "Optionen" konfiguriert wurde. (VirusBarrier X6 wartet, ob noch andere Eindringversuche stattfinden, bevor die E-Mail gesendet wird.)

Wenn Sie eine E-Mail-Benachrichtigung wünschen, müssen Sie Ihre E-Mail-Einstellungen so konfigurieren, dass Sie alle Warnmeldungen per E-Mail empfangen. Klicken Sie hierzu im Abschnitt für Richtlinien auf "Optionen" und dann auf die Schaltfläche "Konfigurieren...".

Sie müssen die E-Mail-Adressen für den Absender und den oder die Empfänger und den Namen des SMTP-Servers (für ausgehende E-Mail-Nachrichten) eingeben. Zudem müssen Sie einen Benutzernamen und ein Passwort eingeben, die Ihr Mailserver akzeptiert. E-Mails können an mehrere Empfänger versendet werden. Klicken Sie auf die Schaltfläche "+, um einen Empfänger hinzuzufügen. Klicken Sie auf die Schaltfläche -, um einen Empfänger zu löschen.

Beispiele für Warnmeldungen

Das folgende Beispiel zeigt eine Warnmeldung, wenn das runde Optionsfeld "In gesperrten Adressen ablegen" markiert und wenn das Kontrollkästchen "Transparentes Fenster anzeigen" aktiviert ist. (Die IP-Adresse wird verschwommen angezeigt.)

Wie Sie sehen, haben Sie keine Wahlmöglichkeit, Sie erhalten nur eine Meldung. Wenn das Kontrollkästchen

"Transparentes Fenster anzeigen" nicht aktiviert wäre, würden Sie gar nichts sehen und VirusBarrier X6 würde die IP-Adresse im Hintergrund der Liste mit gesperrten Adressen hinzufügen.

Das folgende Beispiel zeigt eine Warnmeldung, wenn das runde Optionsfeld "Fragen" markiert und wenn das Kontrollkästchen "Dialogfeld in den Vordergrund bringen" aktiviert ist.

VirusBarrier X6
Warnmeldung: Verbotene ausgehende Daten
Vom Host:
Diesen Host in die gesperrten Adressen aufnehmen
∞
Permanent
Weitere Informationen...
Ignorieren
Gesperrte Adressen
Wann: Donnerstag, 17. Dezember 2009 13:45:00 Europe/Berlin +0100
Details: VirusBarrier sperrte soeben das Versenden geschützter Daten. Wenn Sie diese Daten tatsächlich versenden möchten, klicken Sie bitte auf die Schaltfläche "Ignorieren". Andernfalls werden die Daten nicht versendet und die IP-Nummer des Adressats wird der Liste mit gesperrten Adressen hinzugefügt.

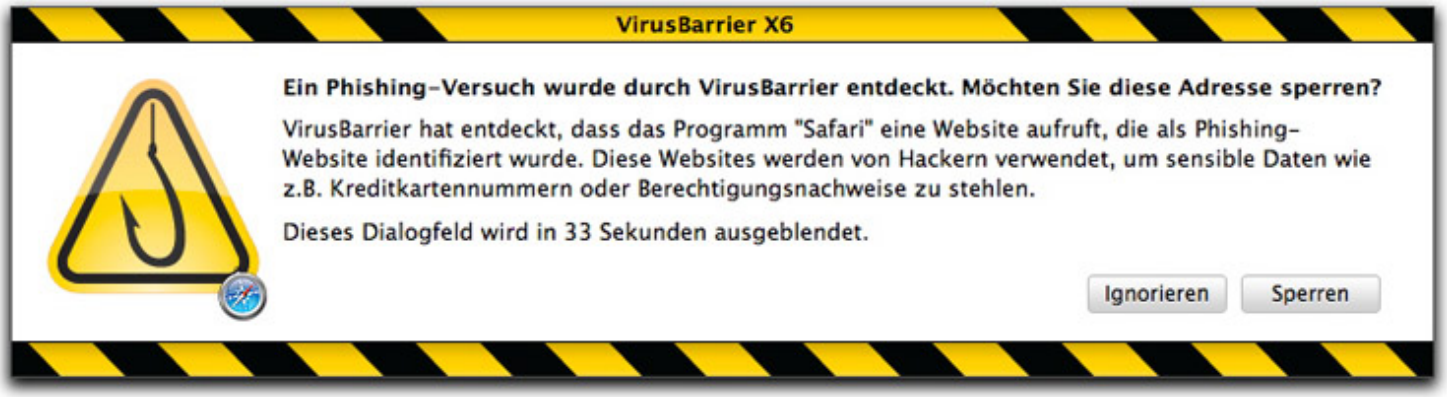
In der oberen Zeile sehen Sie den Grund der Warnmeldung. Der Host (hier verschwommen dargestellt) wird als IP-Adresse angezeigt. Sie können den zugewiesenen Domänennamen (sofern vorhanden) jedoch herausfinden, indem Sie auf das Fragezeichensymbol klicken. Wir haben bereits auf das kleine Dreieck geklickt, um weitere Informationen anzeigen zu lassen. Diese geben weitere Einzelheiten und Anweisungen an.

Durch Klicken auf eine der beiden Schaltflächen auf der unteren rechten Seite können Sie festlegen, was nun geschehen soll.

- **Ignorieren**: Wenn Sie auf diese Schaltfläche klicken, werden die Daten von Ihrem Computer gesendet. Die Datenübertragung wird wie gewöhnlich fortgesetzt, bis VirusBarrier X6 einen weiteren Eindringversuch erkennt. In diesem Fall wird eine weitere Warnmeldung angezeigt.
- **Gesperrte Adressen**: Wenn Sie auf diese Schaltfläche klicken, wird die Datenübertragung verweigert und der Eindringversuch wird gesperrt. Das Datenpaket wird in diesem Fall ignoriert, als wären die Daten niemals übertragen worden. Wenn das empfangene Datenpaket Bestandteil einer Datei ist, so wird diese ebenfalls von Ihrem Computer ignoriert. Wenn das empfangene Datenpaket ein Befehl ist, wird er ebenfalls ignoriert und nicht ausgeführt. Zudem wird die IP-Nummer des Computers, der das Datenpaket an Ihren Computer gesandt hatte, automatisch in die Liste mit gesperrten Adressen aufgenommen und in dieser für den festgelegten Standard-Zeitraum gespeichert. Dieser Zeitraum kann im Popup-Menü geändert werden.

Hier zeigen wir noch ein Beispiel für eine Warnmeldung, die angezeigt wird, wenn ein Programm versucht hat, auf das Internet zuzugreifen und dabei eine Anti-Spyware-Regel verletzt hat.

Schließlich zeigen wir hier eine Art von Warnmeldung die Ihnen angezeigt wird, wenn VirusBarrier X6 einen Phishing-Versuch vereitelt hat. Sie können die Seite sperren oder die Warnmeldung ignorieren und die Seite besuchen – letzteres jedoch auf eigene Verantwortung.


VirusBarrier X6
Ein Phishing-Versuch wurde durch VirusBarrier entdeckt. Möchten Sie diese Adresse sperren?
VirusBarrier hat entdeckt, dass das Programm "Safari" eine Website aufruft, die als Phishing-Website identifiziert wurde. Diese Websites werden von Hackern verwendet, um sensible Daten wie z.B. Kreditkartennummern oder Berechtigungsnachweise zu stehlen.
Dieses Dialogfeld wird in 33 Sekunden ausgeblendet.
Ignorieren
Sperren

© 2009 Intego. Alle Rechte vorbehalten.

So verwenden Sie die Überwachungstools von VirusBarrier X6

- Das VirusBarrier X6-Protokoll
- Monitore für den Datenverkehr
- Ansehen der aktiven Dienste
- Ansehen der Netzwerkinformationen
- Whois-Anfragen
- Traceroute-Suchen

Zum Hauptinhaltsverzeichnis wechseln

VirusBarrier X6 enthält eine Anzahl von Überwachungstools, mit denen Sie sehen können, welche Aktionen ein Programm an schädlicher Software durchgeführt hat, die die Netzwerkaktivitäten und Eindringversuche aufzeichnen und die Ihnen einen Überblick über die Aktivitäten Ihres Macs in Echtzeit geben. Vom Protokoll, das Ihnen sowohl die Ergebnisse der Suche nach schädlicher Software als auch die Netzwerkaktivität anzeigt, bis zum Monitor für den Datenverkehr von VirusBarrier, der den aktuellen Netzwerk-Datendurchsatz anzeigt, helfen Ihnen diese Tools und andere Ihren Mac und seine Netzwerkaktivitäten zu verwalten.

Das VirusBarrier X6-Protokoll

Öffnen Sie das VirusBarrier X6-Protokoll, indem Sie auf das kleine Lupensymbol am unteren Bildschirmrand klicken. Wählen Sie dann Fenster > Protokolle oder drücken Sie Befehlstaste-Wahltaste-L.

Wenn das Protokoll-Fenster angezeigt wird, sehen Sie oben links zwei Schaltflächen: Schädliche Software und Netzwerk. Sie können sich jedes dieser beiden Protokolle anzeigen lassen, indem Sie auf die entsprechende Schaltfläche klicken.

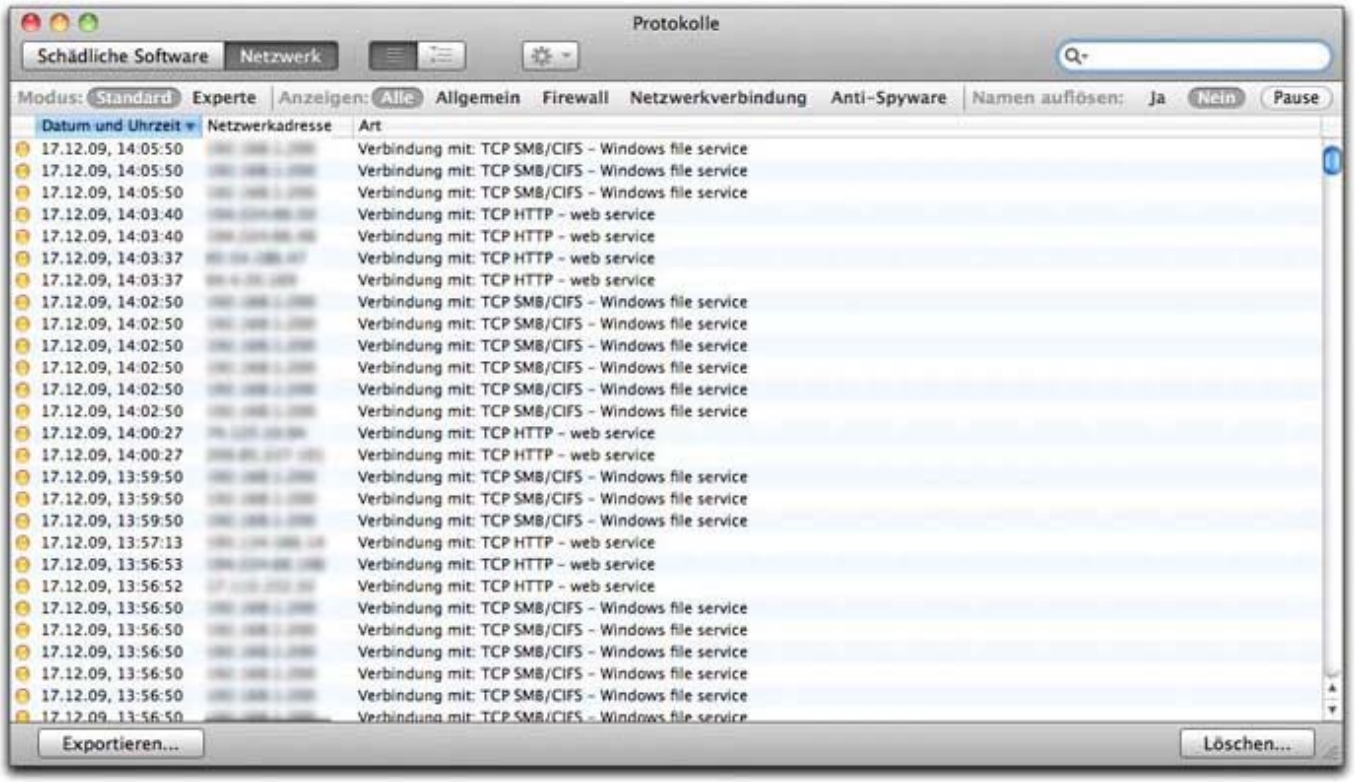
Das Netzwerk-Protokoll

Das Netzwerk-Protokoll zeigt eine Aufzeichnung aller Netzwerkaktivitäten an, die VirusBarrier X6 beobachtet hat,

sowie alle von VirusBarrier X6 blockierten Eindringversuche. Sie können auf das Protokoll Filter nach verschiedenen Kriterien anwenden, um die für Sie interessanten Probleme zu markieren.

Wenn Sie auf das Netzwerk-Protokoll zugreifen möchten, klicken Sie auf die Schaltfläche "Netzwerk" in der oberen linken Ecke des Protokoll-Fensters, wenn es noch nicht ausgewählt ist.

Daraufhin wird Ihnen das Fenster für das Netzwerk-Protokoll angezeigt. Ihr Einträge unterscheiden sich selbstverständlich von den hier angezeigten. Ihre Einträge geben stattdessen die Aktivitäten auf Ihrem Mac wieder, seit Sie VirusBarrier X6 installiert haben (oder seitdem Sie das Protokoll das letzte Mal gelöscht haben).


Protokolle
Schädliche Software
Netzwerk
Modus: Standard Experte
Anzeigen: Alle Allgemein Firewall Netzwerkverbindung Anti-Spyware
Namen auflösen: Ja Nein Pause
Datum und Uhrzeit
Netzwerkadresse
Art
17.12.09, 14:05:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 14:05:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 14:05:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 14:03:40 Verbindung mit: TCP HTTP - web service
17.12.09, 14:03:40 Verbindung mit: TCP HTTP - web service
17.12.09, 14:03:37 Verbindung mit: TCP HTTP - web service
17.12.09, 14:03:37 Verbindung mit: TCP HTTP - web service
17.12.09, 14:02:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 14:02:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 14:02:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 14:02:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 14:02:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 14:02:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 14:00:27 Verbindung mit: TCP HTTP - web service
17.12.09, 14:00:27 Verbindung mit: TCP HTTP - web service
17.12.09, 13:59:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 13:59:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 13:59:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 13:57:13 Verbindung mit: TCP HTTP - web service
17.12.09, 13:56:53 Verbindung mit: TCP HTTP - web service
17.12.09, 13:56:52 Verbindung mit: TCP HTTP - web service
17.12.09, 13:56:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 13:56:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 13:56:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 13:56:50 Verbindung mit: TCP SMB/CIFS - Windows file service
17.12.09, 13:56:50 Verbindung mit: TCP SMB/CIFS - Windows file service
Exportieren...
Löschen...

Ansichtsoptionen für das Netzwerk-Protokoll

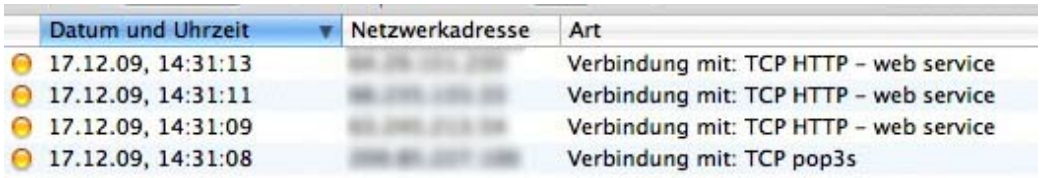
Die obere Hälfte des Protokollfensters enthält drei Gruppen von Optionen, die Auswirkungen darauf haben, wie das Protokoll angezeigt wird.

- Die erste Gruppe dient dem Wechsel zwischen der Standard-Ansicht und der erweiterten Experten-Ansicht.
- Die zweite Gruppe zeigt Teilsätze der Protokollaktivität an, damit Sie potentielle Probleme deutlicher erkennen können.
- Mit der dritten Gruppen können Sie auswählen, ob Sie sich lieber die IP-Adressen oder mithilfe der DNS-Abfrage die Domänennamen anzeigen lassen möchten.

Wir werden jede dieser Gruppe von Optionen einzeln betrachten.

Die Protokollansichten "Standard" und "Experte"

Standard: Die Standardansicht für das Protokollfenster Diese Ansicht zeigt nur vier Informationen für jeden Protokolleintrag an.



Datum und Uhrzeit	Netzwerkadresse	Art
17.12.09, 14:31:13		Verbindung mit: TCP HTTP - web service
17.12.09, 14:31:11		Verbindung mit: TCP HTTP - web service
17.12.09, 14:31:09		Verbindung mit: TCP HTTP - web service
17.12.09, 14:31:08		Verbindung mit: TCP pop3s

- Die Art der Aktivität, angezeigt durch die Farbe des Punktes:
    - Gelb: Beachtenswertes Ereignis, z.B. eine ausgehende Verbindung, eine fehlerhafte Anmeldung, gesperrte ausgehende Daten etc.
    - Rot: Netzwerkangriffe, Sperren von Adressen aus der Liste mit gesperrten Adressen, Sperren von Spyware etc.
- **Datum und Uhrzeit** der Aktivität, entsprechend der Uhrzeiteinstellung auf Ihrem Mac.
- **Netzwerkadresse**, standardmäßig als IP-Adresse angezeigt. Wenn Sie das Kontrollkästchen "Namen auflösen" (siehe unten) markiert haben, sehen Sie die Domänennamen der Adressen, die VirusBarrier X6 auf der Basis der zugehörigen IP-Nummern ermitteln konnte.
- **Art**, kurze Beschreibung der Aktivität.

Experte: Eine erweiterte Ansicht, die - sofern anwendbar - die folgenden Felder anzeigt:

Datum und Uhrzeit	Quelle	Ziel	Protokoll	Quell-Port	Ziel-Port	Markierungen	Schnittstelle	Art
17.12.09, 14:36:28			TCP	55836	80	S	en1	Ausgehende Verbindung
17.12.09, 14:36:28			TCP	55835	80	S	en1	Ausgehende Verbindung
17.12.09, 14:36:28			TCP	55832	80	S	en1	Ausgehende Verbindung
17.12.09, 14:36:27			TCP	55818	995	S	en1	Ausgehende Verbindung

- **Quelle**, die IP-Nummer des Computers (oder Domäne), der die Verbindung herstellte. Für die meisten Aktivitäten wird die Quelle die IP-Adresse Ihres Macs sein. Bei Angriffen oder eingehenden Verbindungen jedoch wird es die Adresse des Remote-Computers sein. Wenn Sie das Kontrollkästchen "Namen auflösen" markiert haben, sehen Sie die Domänennamen der Computer, die VirusBarrier X6 auf der Basis der zugehörigen IP-Nummern ermitteln konnte.
- **Ziel**, standardmäßig als IP-Adresse angezeigt.
- **Protokoll** das beschreibt, wie die Verbindung hergestellt werden sollte: z.B. TCP, UDP, ICMP oder IGMP.
- **Quell-Port**, der Port, von dem die Daten gesendet wurden.
- **Ziel-Port**, der beabsichtigte Port für die Daten.
- **Markierungen** oder TCP-Markierungen: A (Acknowledge = quittieren), S (Synchronize = Synchronisation), F (end of data = Ende der Daten) oder R (Reset = zurücksetzen).
- **Schnittstelle**, die Netzwerkschnittstelle, die zum Senden der Daten verwendet wurde, beispielsweise Ethernet oder AirPort, durch den BSD-Namen angezeigt.
- **Art**, kurze Beschreibung der Aktivität.

Ansehen der Teilsätze des Netzwerk-Protokolls

Aktivitäten lassen sich in vier Gruppen aufteilen: Allgemein, Firewall, Netzwerkverbindungen und Anti-Spyware. Sie können sich entweder alle Aktivitäten für alle Gruppen auf einmal anzeigen lassen oder Sie lassen sich nur die Aktivitäten für eine bestimmte Gruppe anzeigen. Klicken Sie auf eine der Schaltflächen, um die Protokollansicht zu wechseln.

- **Alle**: Alle Aktivitäten, die VirusBarrier X6 verfolgt. Dies ist die Standardeinstellung.
- **Allgemein**: Aktivitäten, die mit der Ausführung von VirusBarrier X6 selbst in Verbindung stehen, wie

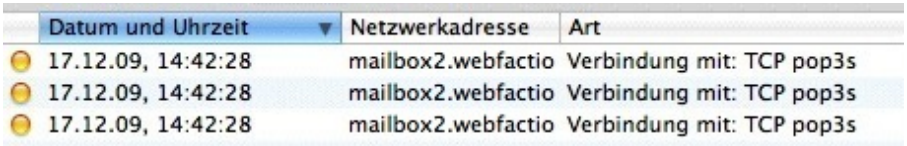
beispielsweise Instanzen beim Starten und Beenden des Programms, zu Anti-Spyware hinzugefügte Programme, in die Liste mit gesperrten Adressen oder in die Liste mit vertrauenswürdigen Adressen eingegebene Elemente usw.

- **Firewall**: Fälle, in denen durch die Netzwerkaktivität eine Firewall-Regel aktiv wurde, sofern für diese Regel die Protokollierung aktiviert war. Aufzeichnungen über Angriffe durch ein Trojanisches Pferd werden ebenfalls im Protokoll angezeigt, sofern Sie den Schutz vor Trojanischen Pferden aktiviert haben.
- **Netzwerkverbindung**: Alle Verbindungen mit Netzwerken oder dem Internet, und wenn Computer mit gesperrten IP-Adressen versuchen, eine Verbindung mit Ihrem Computer herzustellen.
- **Anti-Spyware**: Ein Teilsatz der Gruppe "Allgemein", die nur anzeigt, wenn Programme zur Anti-Spyware-Liste hinzugefügt oder davon entfernt werden oder wenn die Anti-Spyware-Regeln zum Einsatz kommen.

Auflösen von Domänennamen im Netzwerk-Protokoll

Mit VirusBarrier X6 können Sie Eindringlinge verfolgen, indem Sie die Domänennamen anderer Computer auflösen. Internet-Adressen kommen in zwei unterschiedlichen Formaten vor: IP-Nummern, wie z.B. `192.168.1.1` und Namen, wie z.B. `beispiel.com`. Die Korrespondenz zwischen beiden wird in Domänennamenservern über das Internet aufgezeichnet.

Wenn das Kontrollkästchen "Namen auflösen" auf der Registerkarte "Protokoll" markiert ist, versucht VirusBarrier X6, die Domänennamen aller im Protokoll enthaltenen IP-Nummern aufzulösen. Wenn VirusBarrier X6 diese Informationen findet, zeigt das Programm sie als Namen und nicht als Zahlen an.



VirusBarrier X6 ist nicht in der Lage, die Namen aller Internetadressen aufzulösen, da nicht all diesen Adressen Domänennamen zugeordnet sind.

Kontextmenü des Netzwerk-Protokollfensters

Wenn Sie bei gedrückter Taste "ctrl" auf der Tastatur Ihres Macintosh auf einen Protokolleintrag klicken, wird ein Kontextmenü geöffnet.

Dies enthält folgende Optionen:

- **In Zwischenablage kopieren**: Kopiert sichtbare Spalten aus diesem Protokolleintrag in einem durch Tabulatoren getrennten Textformat in die Zwischenablage von Mac OS X. Anschließend können Sie den Inhalt der

Zwischenablage in ein Dokument jedes beliebigen Anwendungsprogramms einsetzen.

- **Quelle in Zwischenablage kopieren**: Kopiert nur das Quellfeld dieses Protokolleintrags in die Zwischenablage von Mac OS X: Steht nur zur Verfügung, wenn Sie das Protokoll im Expertenmodus ansehen.
- **Ziel in Zwischenablage kopieren**: Kopiert nur das Zielfeld dieses Protokolleintrags in die Zwischenablage von Mac OS X: Steht nur zur Verfügung, wenn Sie das Protokoll im Expertenmodus ansehen.
- **Zu vertrauenswürdigen Adressen hinzufügen**: Fügt diese IP-Adresse dauerhaft den Vertrauenswürdigen Adressen hinzu. So werden künftige Datenübertragungen von dieser Adresse ungeachtet der Antivandalismus-Einstellungen erlaubt. Die Firewall von VirusBarrier X6 wird jedoch weiterhin auf die Datenübertragungen von dieser IP-Adresse angewendet.
- **Zu gesperrten Adressen hinzufügen**: Fügt diese IP-Adresse dauerhaft den Gesperrten Adressen hinzu. So werden künftige Datenübertragungen von dieser Adresse ungeachtet der Antivandalismus-Einstellungen unterbunden.
- **Domäneninformationen suchen**: Öffnet das Whois-Fenster von VirusBarrier X6 und führt eine Anfrage nach der ausgewählten IP-Adresse durch. Weitere Informationen erhalten Sie unter Whois-Anfragen.
- **Route suchen**: Öffnet das Traceroute-Fenster von VirusBarrier X6 und führt eine Suche nach der ausgewählten IP-Adresse durch. Weitere Informationen erhalten Sie unter Traceroute-Suchen.
- **In Google Earth anzeigen**: Startet das Programm Google Earth, sofern Sie es installiert haben, und versucht, den geografischen Ort der ausgewählten IP-Adresse zu finden.

Filtern von Daten im Netzwerk-Protokollfenster

Am oberen Rand der Symbolleiste im Protokollfenster gibt es ein Suchfeld zum Filtern von Daten im Protokollfenster nach bestimmten Kriterien. Es werden dann die Einträge angezeigt, die die ausgewählten Kriterien aus den folgenden Kategorien enthalten:

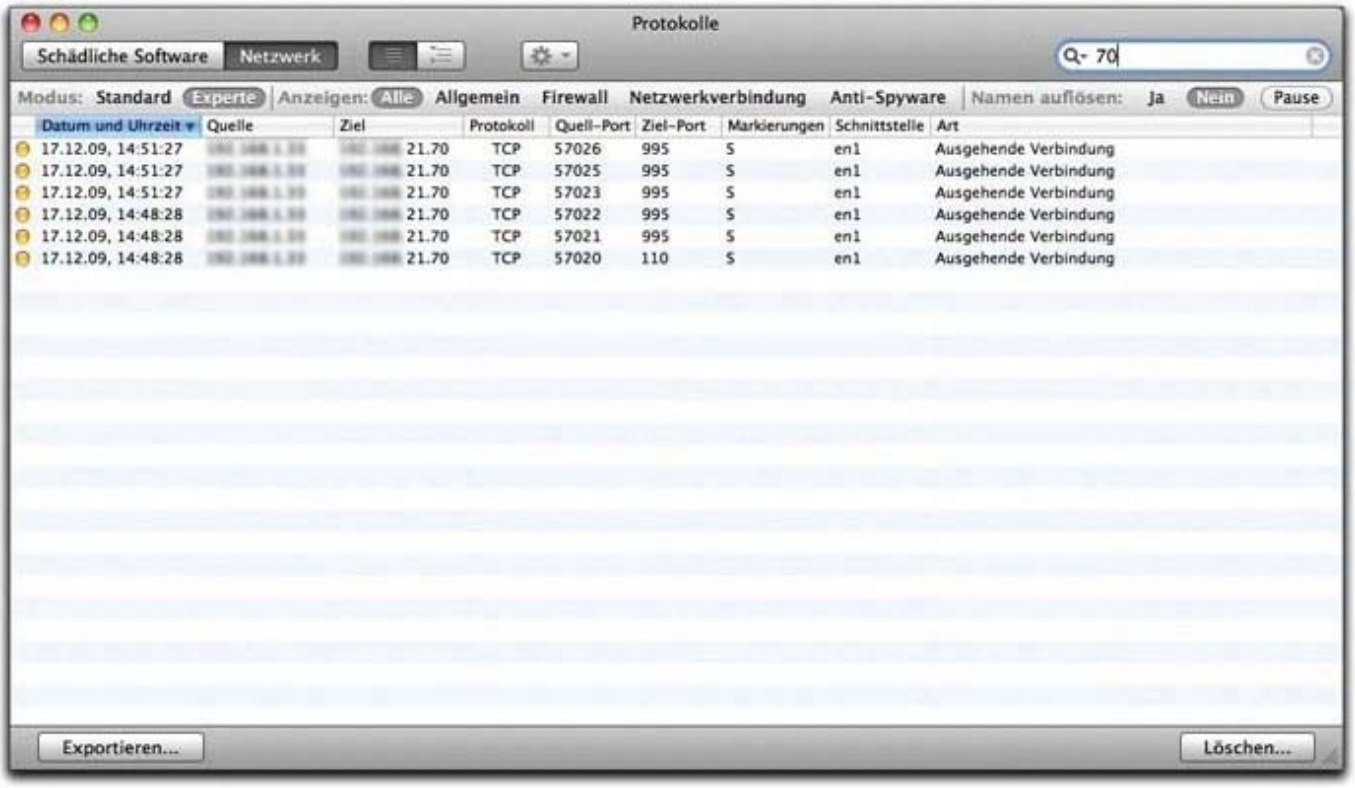
- **Quelladresse**
- **Zieladresse**
- **Quell-Port**
- **Ziel-Port**
- **Schnittstelle**
- **Protokoll**

Die Quelladresse ist das Standardkriterium, wie im Suchfeld angezeigt.

Wenn Sie nach Protokolleinträgen suchen wollen, von denen diese Kriterien erfüllt werden, müssen Sie auf das Schließdreieck neben der Schaltfläche "Suchen" klicken.

Wählen Sie das gewünschte Suchkriterium und geben Sie eine Zeichenfolge in das Feld für die Eingabe des Suchbegriffs ein. Sie müssen nicht den gesamten Suchbegriff eingeben. Mit der Eingabe jedes weiteren Zeichens des Suchbegriffs wird die Anzahl der angezeigten Protokolleinträge entsprechend verringert.

Im Beispiel unten suchen wir nach "70" in der Zieladresse. Der Suchtext kann an einer beliebigen Stelle im Feld auftauchen, nicht nur am Anfang. Die Suche funktioniert auch dann, wenn Sie sich das Protokoll im Standardmodus ansehen. Das Suchfeld ist dann ausgeblendet (in diesem Fall das Ziel).



Wenn Sie den Inhalt des Suchfelds löschen wollen, um eine neue Suche zu starten, müssen Sie auf die Schaltfläche mit dem kleinen "x" im Suchfeld klicken.

Das Protokoll für schädliche Software

Das Protokoll für schädliche Software zeigt eine Aufzeichnung der Aktivitäten schädlicher Software an, die VirusBarrier X6 beobachtet hat. Dazu zählen auch alle manuellen und geplanten Scanvorgänge und deren Ergebnisse. Wie beim

Netzwerk-Protokoll können Sie das Protokoll filtern, um die Probleme zu markieren, die Sie interessieren.

Öffnen Sie das Protokoll für schädliche Software, indem Sie auf das kleine Lupensymbol am unteren Bildschirmrand klicken. Wählen Sie dann Fenster > Protokolle oder drücken Sie Befehlstaste-Wahltaste-L.

Klicken Sie dann auf die Schaltfläche "Schädliche Software" in der oberen linken Ecke, sofern es noch nicht ausgewählt ist.

Das Protokoll sieht wie folgt aus, obwohl Ihr Protokoll natürlich andere Einträge enthält.

Protokolle
Schädliche Software
Netzwerk
Filter
Anzeigen:
Informationen
Warnmeldungen
Gefahren
Pause
Datum und Uhrzeit
Kommentar
Benutzer
18.12.09 12:26:59 Datei 'eicar.com' wurde der Quarantänezone hinzugefügt intego (501)
18.12.09 12:26:57 Scanvorgang auf 'Library' abgeschlossen, Virus wurde dabei entdeckt (gescannt: 1.475, infiziert: 1, besc... intego (501)
18.12.09 12:26:54 Virus 'Multi/Eicar' in Datei 'eicar.com' entdeckt intego (501)
18.12.09 12:26:54 Scanvorgang startete auf 'Library' root (0)
18.12.09 12:26:53 Scanvorgang auf 'Computer' angehalten intego (501)
18.12.09 12:26:48 Scanvorgang startete auf 'Computer' root (0)
18.12.09 12:25:33 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:32 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:32 Echtzeit-Scanner wird angehalten root (0)
18.12.09 12:25:31 Vdef-Aktualisierung (Virendefinition vom 18.12.09) root (0)
18.12.09 12:25:31 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:30 Echtzeit-Scanner wird angehalten root (0)
18.12.09 12:25:29 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:29 Echtzeit-Scanner wird gestartet root (0)
Exportieren...
Löschen...

Sie können sich die Protokollinformationen auf zwei Arten anzeigen lassen. Im obigen Beispiel werden die Protokolleinträge in einer linearen Reihenfolge angezeigt, wobei ein Eintrag eine Zeile belegt. Sie können oben links im Fenster auf die zweite Schaltfläche klicken und die Protokolleinträge in hierarchischer Reihenfolge anzeigen. Hierbei werden verwandte Einträge unter Schließdreiecken gruppiert:

Protokolle
Schädliche Software
Netzwerk
Filter
Anzeigen:
Informationen
Warnmeldungen
Gefahren
Pause
Datum und Uhrzeit
Kommentar
Benutzer
18.12.09 12:26:59 Datei 'eicar.com' wurde der Quarantänezone hinzugefügt intego (501)
18.12.09 12:26:48 Scanvorgang von 'Computer' (gescannt: 1.475, infiziert: 1, beschädigt: 0, repariert: 0) intego (501)
18.12.09 12:26:57 Datei 'eicar.com' wurde der Quarantänezone hinzugefügt
18.12.09 12:26:48 Scanvorgang auf 'Library' abgeschlossen, Virus wurde dabei entdeckt (gescannt: 1.475, infiziert: 1, besc...
18.12.09 12:26:54 Virus 'Multi/Eicar' in Datei 'eicar.com' entdeckt
18.12.09 12:26:54 Scanvorgang startete auf 'Library'
18.12.09 12:26:53 Scanvorgang auf 'Computer' angehalten intego (501)
18.12.09 12:26:48 Scanvorgang startete auf 'Computer' root (0)
18.12.09 12:25:33 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:32 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:32 Echtzeit-Scanner wird angehalten root (0)
18.12.09 12:25:31 Vdef-Aktualisierung (Virendefinition vom 18.12.09) root (0)
18.12.09 12:25:31 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:30 Echtzeit-Scanner wird angehalten root (0)
18.12.09 12:25:29 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:29 Echtzeit-Scanner wird gestartet root (0)
Exportieren...
Löschen...

Das Protokoll wird bei folgenden Ereignissen angezeigt:

- Sie starten einen Scanvorgang
- Sie brechen einen Scanvorgang ab
- Sie Starten oder Stoppen den Echtzeit-Scanner
- VirusBarrier X6 hat einen Scanvorgang beendet, mit Ergebnis
- VirusBarrier X6 hat einen Virus erkannt
- VirusBarrier X6 hat eine beschädigte Datei erkannt
- VirusBarrier X6 repariert eine infizierte Datei
- Dateien werden der Quarantänezone hinzugefügt oder aus ihr entfernt
- Dateien werden der Liste mit vertrauenswürdigen Dateien hinzugefügt oder aus ihr entfernt
- Virusdefinitionen werden aktualisiert

Die farbigen Punkte in Spalte ganz links zeigen Ihnen an, welche Arten von Einträgen im Protokoll angezeigt werden. Grüne Punkte stehen für Informationen, z. B. das Starten des Echtzeit-Scanners oder das Aktualisieren der Virusdefinitionen. Orangene Punkte stehen für Warnungen, z. B. das Stoppen des Echtzeit-Scanners. Rote Punkte stehen für Gefahren, z. B., wenn mit einem Virus infizierte oder beschädigte Dateien gefunden werden. Die für den Scanvorgang ausgewählten Dateien, Ordner und Datenträger sind benannt – ebenso wie alle aufgetretenen Probleme.

Sie können auswählen, dass nur bestimmte Arten von Informationen angezeigt werden, indem Sie auf eine der drei Schaltflächen für den Protokolltyp klicken und so die entsprechenden Einträge ein- oder ausblenden.

Protokolle
Schädliche Software
Netzwerk
Filter
Anzeigen:
Informationen
Warnmeldungen
Gefahren
Pause
Datum und Uhrzeit
Kommentar
Benutzer
18.12.09 12:26:59 Datei 'eicar.com' wurde der Quarantänezone hinzugefügt intego (501)
18.12.09 12:26:48 Scanvorgang von 'Computer' (gescannt: 1.475, infiziert: 1, beschädigt: 0, repariert: 0) intego (501)
18.12.09 12:26:57 Datei 'eicar.com' wurde der Quarantänezone hinzugefügt
18.12.09 12:26:48 Scanvorgang auf 'Library' abgeschlossen, Virus wurde dabei entdeckt (gescannt: 1.475, infiziert: 1, besc...
18.12.09 12:26:54 Virus 'Multi/Eicar' in Datei 'eicar.com' entdeckt
18.12.09 12:26:54 Scanvorgang startete auf 'Library'
18.12.09 12:26:53 Scanvorgang auf 'Computer' angehalten intego (501)
18.12.09 12:26:48 Scanvorgang startete auf 'Computer' root (0)
18.12.09 12:25:33 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:32 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:32 Echtzeit-Scanner wird angehalten root (0)
18.12.09 12:25:31 Vdef-Aktualisierung (Virendefinition vom 18.12.09) root (0)
18.12.09 12:25:31 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:30 Echtzeit-Scanner wird angehalten root (0)
18.12.09 12:25:29 Echtzeit-Scanner wird gestartet root (0)
18.12.09 12:25:29 Echtzeit-Scanner wird gestartet root (0)
Exportieren...
Löschen...

Wird schädliche Software gefunden, wird sie im Protokoll in einer von vier Kategorien aufgelistet:

- Virus
- Hintertür
- Trojanisches Pferd
- Exploit

Sie können für einige Protokolleinträge Aktionen durchführen. Wählen Sie hierzu diese Einträge aus, und klicken Sie in der Symbolleiste des Protokollfensters auf die Aktionsschaltfläche. Oder klicken Sie mit der rechten Maustaste auf diese Schaltfläche. Im angezeigten Kontextmenü sehen Sie drei Optionen:

abgeschlossen, Virus wurde dabei entdeckt (gescannt: 2.67
Im Finder anzeigen
Vom Datenträger löschen
Verdächtige Datei an Intego senden

- **Im Finder anzeigen**: Mit dieser Option öffnen Sie ein Fenster im Finder, in dem die ausgewählte Datei hervorgehoben wird, damit Sie den Speicherort sehen können. Sie können die Datei dann entweder löschen oder andere Aktionen damit durchführen.
- **Vom Datenträger löschen**: Diese Option ist nur für beschädigte Dateien verfügbar. Wenn Sie diese Option auswählen, wird die beschädigte Datei von Ihrem Datenträger gelöscht.
- **Verdächtige Datei an Intego senden**: Wählen Sie diese Option aus, um verdächtige Dateien an Intego zu senden, damit Sie dort im Virus Monitoring Center untersucht werden können.

Sie können die Suchergebnisse auch filtern, indem Sie in das Suchfeld der Fenstersymbolleiste Text eingeben. Während der Texteingabe wird die Anzahl der Ergebnisse verringert. Es werden nur die Protokolleinträge angezeigt, die den eingegebenen Text enthalten.

Sie können alle Protokollelemente kopieren. Wählen Sie hierzu die Elemente aus, und drücken Sie Befehlstaste-C. Anschließend können Sie diese Elemente in ein anderes Programm einfügen, falls erforderlich.

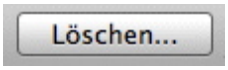
Sie können alle Protokollelemente entfernen, indem Sie diese auswählen und die Löschtaste drücken. Sie können das gesamte Protokoll löschen, indem Sie auf die Schaltfläche "Löschen..." klicken.

Gebräuchliche Funktionen für das Netzwerkprotokoll und das Protokoll für schädliche Software

Pausieren der kontinuierlichen Protokollanzeige

Wenn innerhalb kurzer Zeit viele Verbindungen mit Ihrem Computer hergestellt und beendet werden, kann es problematisch sein, das sich ständig aktualisierende Protokoll zu lesen. Sie können das Protokoll einfacher ansehen, wenn Sie auf die Schaltfläche zum Anhalten in der oberen rechten Ecke des Protokollfensters klicken. Das Protokoll wird angehalten, damit Sie die Daten lesen können. Das Protokoll zeichnet jedoch weiterhin Daten auf und zeigt die neuen Daten an, wenn Sie das Protokoll weiterlaufen lassen. Klicken Sie erneut auf die Schaltfläche "Pause", um wieder die Echtzeitanzeige des Protokolls zu aktivieren.

So löschen Sie das Protokoll



Um alle im Protokoll gespeicherten Informationen zu löschen, müssen Sie nur auf die Schaltfläche "Löschen..." in der unteren rechten Ecke klicken. Nun wird ein Fenster geöffnet, in dem Sie aufgefordert werden, den Löschvorgang zu bestätigen.

Das Protokoll wird auch automatisch gelöscht, wenn Sie das Kontrollkästchen "Protokoll nach dem Exportieren löschen" in den Einstellungen für das Protokoll markiert haben und wenn Sie VirusBarrier X6 so eingerichtet haben, dass regelmäßig ein Protokoll exportiert wird. Weitere Informationen über die Protokolleinstellungen finden Sie unter Einstellungen und Konfigurationen.

So exportieren Sie das Protokoll

Sie können das Protokoll in mehreren Formaten exportieren. Wenn Sie das Protokoll manuell exportieren, werden nur die angezeigten Daten exportiert. Wenn Sie im Protokollfenster z.B. nur Firewall markiert haben, werden nur die Firewall-Daten exportiert. (Sie können die Protokolldaten auch automatisch exportieren lassen. Weitere Informationen über die Protokolleinstellungen finden Sie unter Einstellungen und Konfigurationen.)

Sie können das Protokoll exportieren, indem Sie auf die Schaltfläche "Exportieren..." klicken. Nun wird ein Dialogfeld geöffnet, sodass Sie die Datei speichern können. Hierbei können Sie den Namen der Datei ändern. Wählen Sie den Ort, an dem das Protokoll gespeichert werden sollen. Standardmäßig werden alle exportierten Dateien im Ordner "Dokumente" gespeichert.

ACHTUNG: Es kann einige Minuten dauern bis das Protokoll exportiert ist, wenn die Funktion "Namen auflösen" eingeschaltet ist.

Protokolle können in sechs Formaten exportiert werden: Klicken Sie ins Popup-Menü "Format", um das Exportformat zu wählen.

Dabei handelt es sich um folgende Formate:

- **HTML für Experten**: HTML-Format das alle Spalten anzeigt, die im Expertenmodus sichtbar sind. In diesem Format können Sie den letzten Browserverlauf teilweise zurückverfolgen, da VirusBarrier X6 anklickbare Links liefert für alle Protokolleinträge, die nicht sichere Webseiten betreffen. (Das sind über TCP verbundene Ziel-Ports, die auf die Ports 80 oder 8080 zielen.)
- **Text für Experten**: Durch Tabulatoren getrenntes Nur-Text-Format mit zusätzlichen Spalten, damit im Expertenmodus alle sichtbaren Spalten angezeigt werden können. Dieser Modus eignet sich am besten zum Importieren in eine Tabelle oder ein Datenbankprogramm.
- **HTML**: HTML-Format das alle Spalten anzeigt, die im Standardmodus sichtbar sind. Wie bei HTML für Experten-Exporten können Sie mit diesem Dateiformat den letzten Browserverlauf zurückverfolgen.
- **Analytisch**: Ein Textformat, das dem Format "Text für Experten" ähnelt, wobei allerdings keine Reiter vorhanden sind. Manche Felder sind beschriftet.
- **Text**: Durch Tabulatoren getrenntes Nur-Text-Format mit allen im Standardmodus sichtbaren Spalten.
- **Wer ist da?**: Das Protokoll als Textdatei mit den folgenden Spalten: Datum, Uhrzeit, Ergebnis, Hostname, Server-Port und Methode: hilfreich in einigen Protokollanalyseprogrammen.

Monitore für den Datenverkehr

VirusBarrier X6 verfügt über eine Anzahl von Funktionen, mit denen Sie den ein- und ausgehenden Netzwerkdatenverkehr auf Ihrem Mac überwachen, Anfragen und Suchvorgänge nach Netzwerkadressen durchführen und sehen können, welche Dienste und Netzwerke für Ihren Mac verfügbar sind.

Fenster für den Datenverkehr

Das Fenster für den Datenverkehr enthält einen Satz von Anzeigepegeln für die Aktivität. Er zeigt Ihnen die Art und die Anzahl der Netzwerkaktivitäten an, die sowohl über das Internet als auch über lokale Netzwerke auf Ihrem Mac ein- und ausgehen. Sie können auf das Fenster für den Datenverkehr zugreifen, indem Sie auf das kleine Symbol klicken, das unten angezeigt wird und dann "Fenster > Verkehr" wählen. Sie können auch Befehlstaste-Wahltaste-4 drücken.

Für das Datenverkehrsfenster gibt es vier Ansichtsmodi. Sie können zwischen ihnen hin- und herwechseln, indem Sie auf die kleinen Schaltflächen am oberen Bildschirmrand klicken.

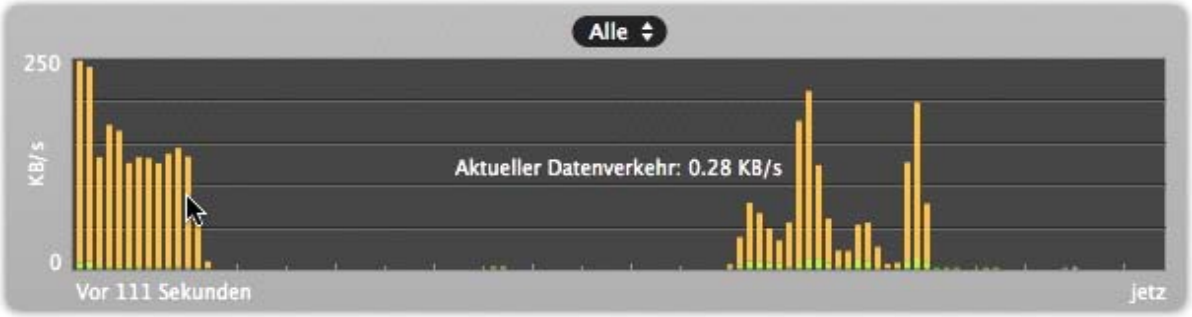
Die erste Schaltfläche ist die Standardansicht und zeigt den Datenverkehr durch zwei Pegelzeilen und eine Zeitlinie an.

Die oberen Pegel "EIN" zeigen Werte standardmäßig in Orange an und geben die Anzahl der eingehenden Daten auf Ihrem Mac wieder. Die Pegel "AUS" in der zweiten Zeile zeigen Werte standardmäßig in Grün an und geben die Anzahl der ausgehenden Daten auf Ihrem Mac wieder. Die Zahl in den Pegeln gibt den aktuellen Datendurchsatz in Kilobyte pro Sekunden (k/s) wieder. Darunter steht die Gesamtzahl, normalerweise in Megabyte (MB) oder Gigabyte (GB).

Die Zeitachse unten zeigt den Datenverkehr im Zeitverlauf an. Die Balken ganz rechts zeigen die Gegenwart an und die linken die Vergangenheit. Wie oben zeigen die orangenen Werte den eingehenden Datenverkehr und die grünen Werte zeigen den ausgehenden Datenverkehr.

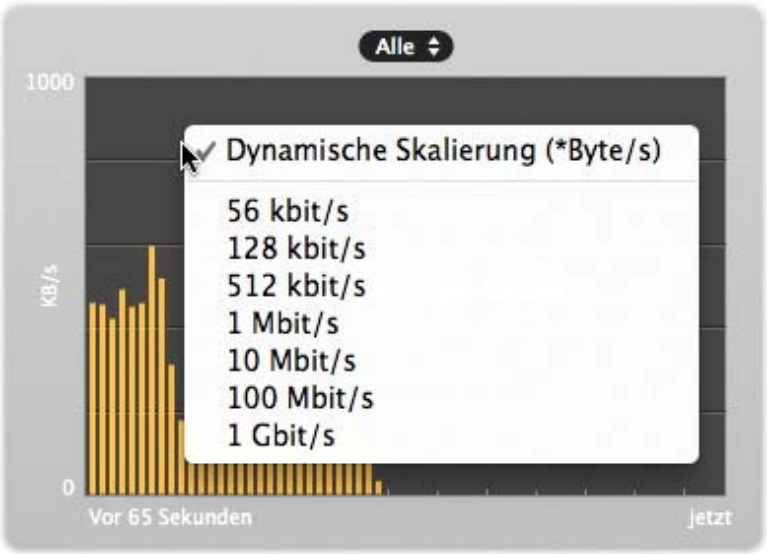
Standardmäßig zeichnet die Zeitachse Aktivitäten der vergangenen 111 Sekunden auf. Sie können den Zeitraum verlängern, indem Sie das Fenster größer ziehen. Klicken Sie hierzu entweder auf die grüne Zoom-Schaltfläche in der oberen linken Ecke oder klicken Sie auf die untere rechte Ecke des Fensters und ziehen Sie das Fenster auf. Die Maximalzeit wird durch die Größe Ihres Bildschirms festgelegt oder dadurch, ob Sie sich jeweils nur einen Bereich der Zeitachse ansehen möchten.

Wenn Sie den Mauszeiger über eine Zeitachse verschieben, wird ein Text angezeigt, aus dem der aktuelle durchschnittliche Datendurchsatz ersichtlich ist. Der Wert des Datendurchsatzes wird einmal pro Sekunde aktualisiert.



Die zweite Ansichtsschaltfläche zeigt den Datenverkehr in drei Zeitachsen an: eine für den eingehenden, eine für den ausgehenden und eine für den gesamten Datenverkehr.

Für diesen Ansichtsmodus gibt es eine Spezialfunktion, mit der Sie die Skala für die Diagramme "Ein" und "Aus" wählen können. Verschieben Sie hierzu die Maus über eines der Diagramme, halten Sie dabei die Steuerungstaste gedrückt und klicken Sie. Daraufhin können Sie in einem Popup-Menü aus mehreren Optionen wählen.



Damit können Sie die korrekte Skalierung der Diagramme für die Anzeige der zu erwartenden Datendurchsätze wählen. Wählen Sie die Option "Dynamische Skalierung", wenn sich die Skalierung der Diagramme, wie zuvor beschrieben, automatisch in Abhängigkeit vom Datendurchsatz ändern soll.

Die dritte Schaltfläche für Ansichtsmodi zeigt den Datenverkehr als Pegelserie in horizontaler Ausrichtung, ohne Zeitachse, an. Die vierte Schaltfläche zeigt die gleichen Pegel, jedoch in vertikaler Ausrichtung (ohne Abbildung).

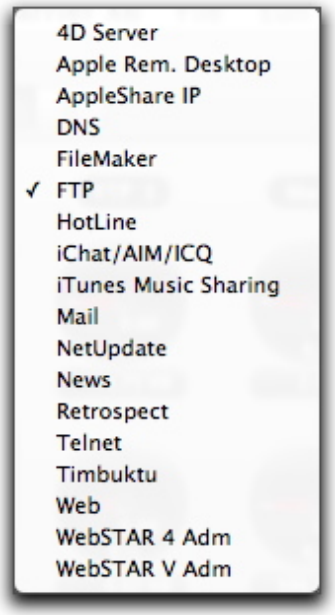
Die drei Ansichten, die runde Pegel enthalten, verfügen zudem über Schaltflächen zum Zurücksetzen. Wenn Sie auf diese Schaltfläche klicken, wird die untere Pegelzeile, die den gesamten Datenverkehr anzeigt, auf Null zurückgesetzt.

Auswählen der Arten von Netzwerkaktivitäten

In jedem Ansichtsmodus können Sie auswählen, welche Arten von Datenverkehr angezeigt werden sollen: Standardmäßig werden die Aktivitäten der Datentypen Web, FTP, Mail und iChat/AIM überwacht. Der fünfte Pegel zeigt jeden weiteren Datenverkehr an und der sechste das Gesamtdatenverkehrsaufkommen.

Sie können jedoch auch auswählen, welche Datentypen für die ersten vier Pegelpaare angezeigt werden sollen. Klicken Sie hierzu auf die Anzeige über einem der Pegel.

Nun können Sie den Typ der Netzwerkaktivitäten auswählen.



Über den Fensterabschnitt für Datenverkehrseinstellungen können Sie dieser Liste Dienste hinzufügen oder welche davon entfernen. Weitere Informationen siehe Einstellungen für den Datenverkehr unter Einstellungen und Konfigurationen.

VirusBarrier Traffic Monitor

Wenn Sie VirusBarrier X6 installieren wird auch ein Programm namens VirusBarrier Traffic Monitor in Ihrem Programmordner platziert. Sie können dieses Programm starten, indem Sie auf das Symbol doppelklicken. Oder Sie wählen aus dem Intego-Menü "VirusBarrier X6 > VirusBarrier Traffic Monitor öffnen".

VirusBarrier Traffic Monitor

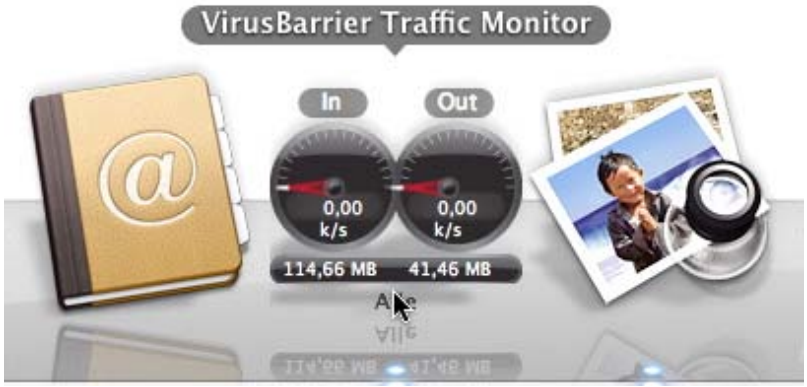
Das Programm VirusBarrier Traffic Monitor öffnet ein kleines, schwebendes Fenster, in dem Sie die Netzwerkaktivitäten ständig überwachen können, ohne die gesamte Palette mit den Anzeigepegeln von VirusBarrier X6 für die Netzwerkaktivitäten geöffnet halten zu müssen.

Nach dem Starten von VirusBarrier Traffic Monitor wird dessen Fenster mit den Anzeigepegeln in der unteren rechten Bildschirmecke angezeigt. Sie können VirusBarrier Traffic Monitor verschieben, indem Sie auf das Fenster klicken und es an eine andere Stelle auf Ihrem Bildschirm ziehen.

Standardmäßig zeigt VirusBarrier Traffic Monitor den gesamten Datenverkehr für alle Dienste an. Sie können ändern, welche Art von Datenverkehr angezeigt wird, indem Sie auf "Alle" unten im Fenster von VirusBarrier Traffic Monitor klicken und aus dem Popup-Menü einen Dienst wählen.

Wenn Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf eine beliebige Stelle im Fenster von VirusBarrier Traffic Monitor klicken, wird ein Popup-Menü mit zwei Optionen geöffnet.

Die Option "Im Dock anzeigen" schließt das Fenster von VirusBarrier Traffic Monitor. Das Symbol von VirusBarrier Traffic Monitor im Dock ändert sich und zeigt an, dass die Anzeigepegel in Echtzeit aktualisiert werden.



Die Netzwerkaktivität wird auch im VirusBarrier Traffic Monitor-Symbol angezeigt. Dieses Symbol wird eingeblendet, wenn Sie zwischen den Programmen wechseln, indem Sie Befehlstaste-Tabulator drücken.

Wenn wieder das Fenster von VirusBarrier Traffic Monitor geöffnet werden soll, müssen Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf das Symbol von VirusBarrier Traffic Monitor im Dock klicken und dann die Menüoption "Im Fenster anzeigen" wählen.

Wenn VirusBarrier Traffic Monitor im Dock angezeigt wird, können Sie die Anzeige ändern, wenn Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf das Symbol von VirusBarrier Traffic Monitor im Dock klicken und aus dem Dock-Menü einen anderen Dienst wählen.

Wenn Sie die Option "Im Dock behalten" wählen, wird das VirusBarrier Traffic Monitor-Symbol dauerhaft im Dock abgelegt. Es bleibt auch dort, wenn das Programm nicht ausgeführt wird. Sie können es dann einfach öffnen, indem Sie auf das Symbol im Dock klicken. Wenn Sie die Option zum Öffnen beim Anmelden wählen, wird das Programm jedes Mal geöffnet, wenn Sie eine Benutzersitzung auf Ihrem Mac beginnen.

Einstellungen für VirusBarrier Traffic Monitor

Mehrere Optionen der Einstellungen haben eine Auswirkung auf das Verhalten von VirusBarrier Traffic Monitor. Sie können diese Einstellungen vornehmen, indem Sie "VirusBarrier Traffic Monitor > Einstellungen" wählen oder Befehlstaste-Komma drücken, während VirusBarrier Traffic Monitor ausgeführt wird.

- **Darstellung**: Wählen Sie "Anzeigepegel", "Thermometer" oder "Licht":

- **Fensterebene**: Wenn Sie die Option "Über anderen Fenstern schweben" wählen, wird VirusBarrier Traffic Monitor immer im Vordergrund angezeigt, vor allen anderen Programmen.
- **Mausverhalten**: Wenn Sie die Option "Mausklicks ignorieren" wählen, können Sie das Fenster von VirusBarrier Traffic Monitor nicht verschieben und die überwachten Dienste nicht ändern.

Das Widget für VirusBarrier Traffic Monitor

VirusBarrier X6 installiert das Widget für VirusBarrier Traffic Monitor. Es wird in das Dashboard von Mac OS X geladen und zeigt Ihnen die Netzwerkaktivität an, wenn Sie im Dashboard sind.

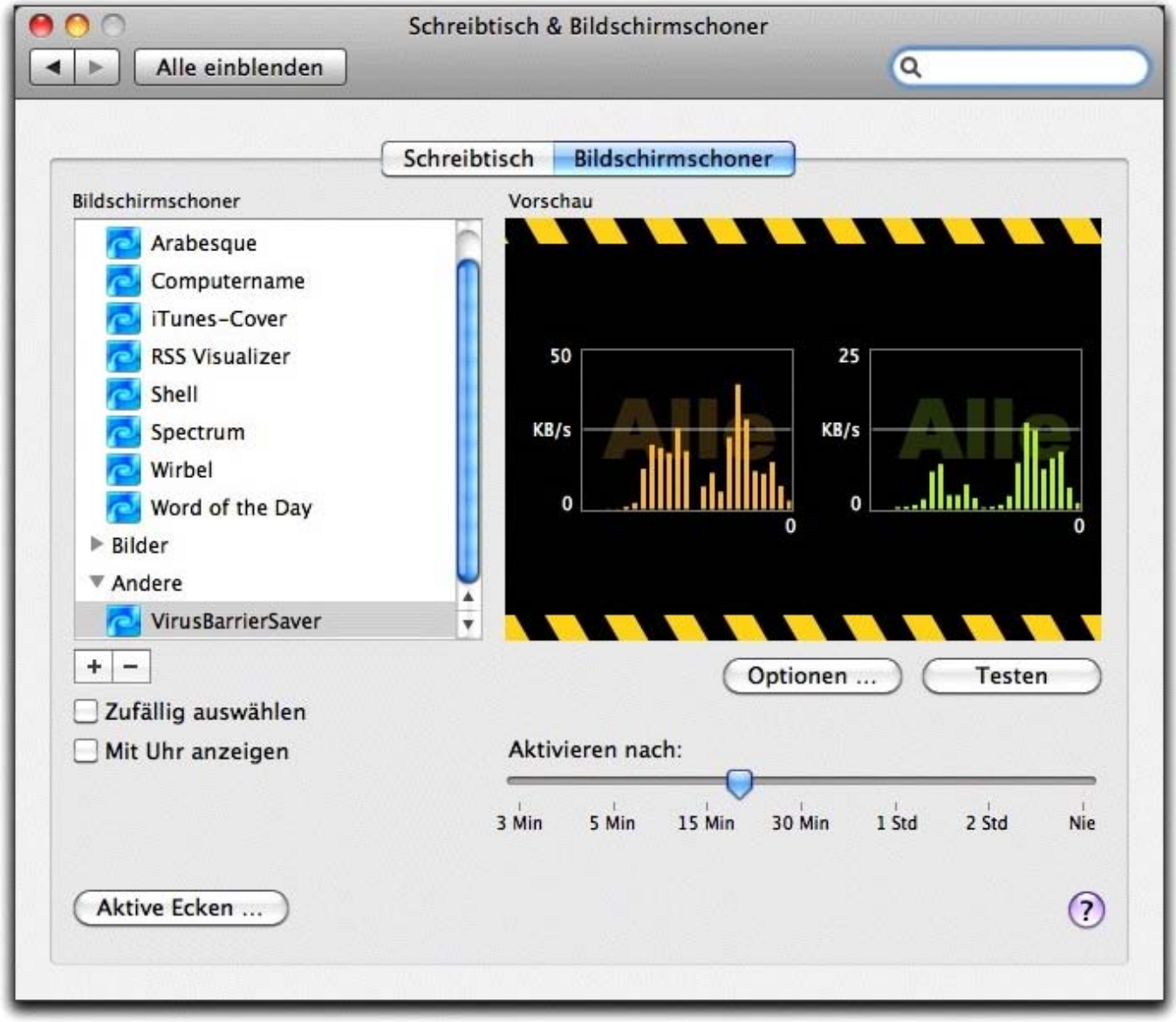
Aktivieren Sie das Dashboard, um sich das Widget für VirusBarrier Traffic Monitor anzeigen zu lassen. Klicken Sie auf die Schaltfläche "+", wenn Sie sich alle auf Ihrem Computer verfügbaren Widgets anzeigen lassen möchten. Wählen Sie VirusBarrier Traffic Monitor aus der Liste. Das Symbol sieht folgendermaßen aus:

Wenn Sie es Ihren aktiven Widgets hinzufügen, können Sie VirusBarrier Traffic Monitor immer dann sehen, wenn Sie in das Dashboard wechseln. Wie beim Programm VirusBarrier Traffic Monitor können Sie das Fenster verschieben oder die Art der angezeigten Aktivitäten ändern.

Der Monitor-Bildschirmschoner von VirusBarrier X6

VirusBarrier X6 installiert einen Bildschirmschoner, der Ihnen einen Überblick über die Netzwerkaktivitäten gibt, wenn Ihr Computer ansonsten nicht verwendet wird. Wenn Ihr Computer als Server betrieben wird, werden Sie durch diesen Bildschirmschoner zudem über die aktuellen Netzwerkaktivitäten informiert.

Wenn Sie den Bildschirmschoner von VirusBarrier X6 verwenden wollen, müssen Sie die Menüoption "Systemeinstellungen..." aus dem Apple-Menü wählen und dann erst auf die Schaltfläche "Schreibtisch & Bildschirmschoner" und dann auf "Bildschirmschoner" klicken. Wählen Sie "VirusBarrierSaver" aus der Liste der Bildschirmschoner.



Der Vorschaubildschirm zeigt nur den gesamten Datenverkehr an. Er zeigt jedoch den Datenverkehr nach einzelnen Diensten an, wenn diese tatsächlich ausgeführt werden. Klicken Sie auf "Optionen" um festzulegen, in welcher Reihenfolge die Dienste angezeigt werden sollen.

Ziehen Sie die Dienste einfach in die gewünschte Reihenfolge. Die Anzahl der darstellbaren Dienste hängt von der Größe Ihres Bildschirms, der verwendeten Auflösung (Anzahl der Bildpunkte in beiden Achsen) und der Anzahl der verwendeten Videomonitore ab. Die wichtigsten sollten daher an erster Stelle stehen.

Weitere Informationen über die Einstellung von Bildschirmschonern finden Sie in der Hilfe zu Mac OS X.

Ansehen der aktiven Dienste

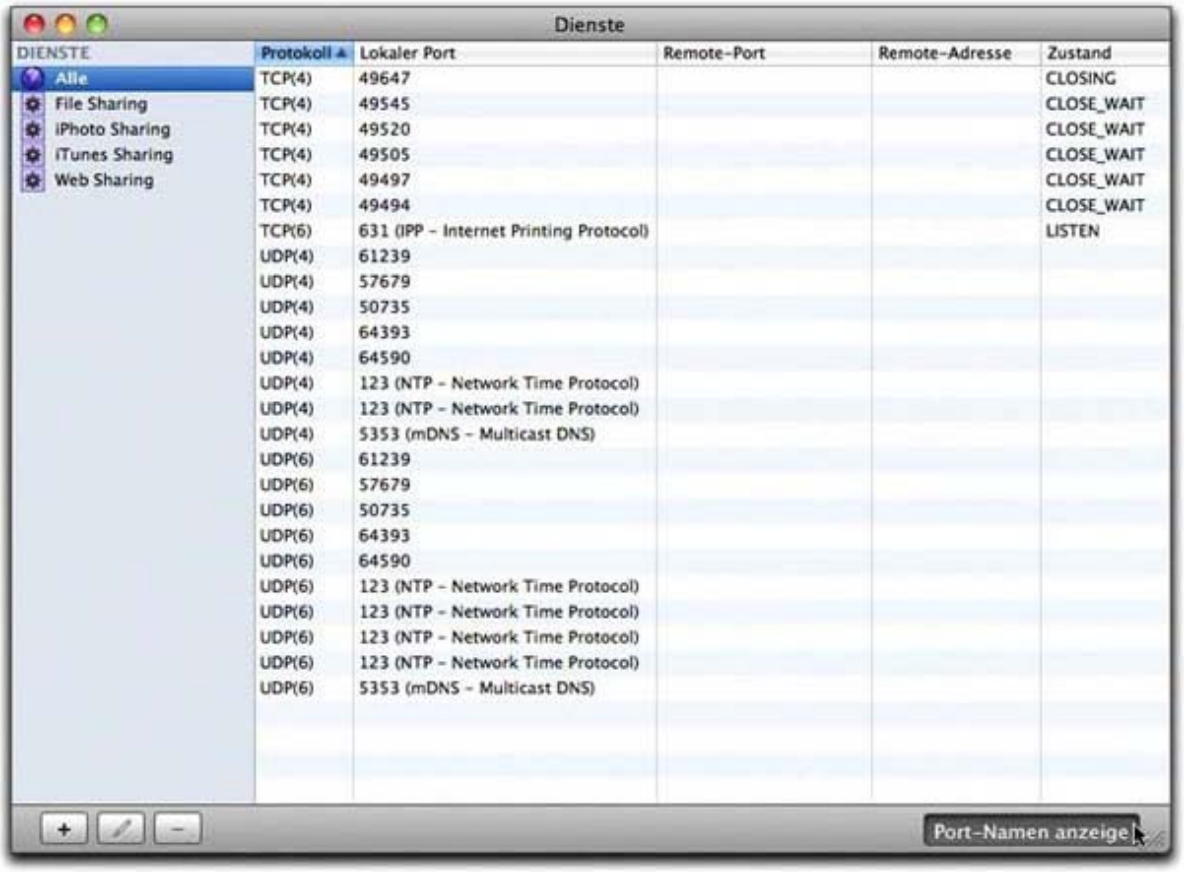
Das Dienstefenster von VirusBarrier X6 zeigt alle aktiven Netzwerkdienste an, die auf Ihrem Computer für andere Benutzer über ein Internetprotokoll erreichbar sind, wie beispielsweise Webserver, Mailserver usw.

Klicken Sie auf das Symbol mit dem Doppelpfeil in der unteren rechten Ecke im Übersichtsfenster von VirusBarrier X6, um sich das Dienstefenster anzeigen zu lassen.

Für jeden verwendeten Port werden die folgenden Informationen angezeigt:

- Das Protokoll (TCP oder UDP)
- Die lokale Portnummer (abhängig vom Protokoll, das sie repräsentiert, wenn es ein Standard-Protokoll ist, wie z.B. Port 21 für FTP)
- Die Remote-Portnummer
- Die Remote-Adresse (die IP-Adresse der Remote-Verbindung)
- Den Verbindungsstatus - z.B. ob die Verbindung aktiv ist oder ob sie nur auf Datenverkehr wartet.

Wenn Sie zusätzlich zu den Portnummern auch die Namen der Ports sehen möchten, klicken Sie auf die Schaltfläche "Port-Namen anzeigen" in der unteren rechten Ecke, wie hier dargestellt.



Da die Liste der Ports, die von allen Diensten verwendet werden, sehr lang sein kann, bietet VirusBarrier X6 Filter an, mit denen Sie sich die Ports anzeigen lassen können, die von bestimmten Diensten verwendet werden. Sie können zwischen File Sharing, iPhoto Sharing, iTunes Sharing und Web Sharing auswählen, indem Sie in die linke Spalte klicken. Sie können aber auch eigene Filter erstellen.

Klicken Sie hierzu auf die Schaltfläche "+" in der unteren linken Ecke des Fensters. Hierauf wird das Dialogfeld "Intelligenter Filter" geöffnet.

Im ersten Popup-Menü können Sie festlegen, ob Sie möchten, dass der Filter mit einer der von Ihnen vorgegebenen Bedingungen übereinstimmt oder mit allen.

Das zweite Popup-Menü legt den Informationstyp fest, den der Filter suchen soll. Die Auswahl entspricht den Spalten im Dienstefenster: Protokoll, lokaler Port, Remote-Port, Remote-Adresse und Zustand. Nachdem Sie eine dieser Optionen ausgewählt haben, können Sie die Filterdetails festlegen. In diesem Beispiel werden nur die Dienste aufgeführt, bei denen der lokale Port in einem bestimmten Rahmen liegt.

Wenn Sie auf das Pluszeichen in der rechten Fensterhälfte klicken, können Sie weitere Bedingungen hinzufügen. Wenn Sie hingegen auf das Minuszeichen neben einer Bedingung klicken, wird diese aus der Liste entfernt. Zudem können Sie Filterbedingungen auch verändern, indem Sie einfach die Option aus dem Popup-Menü ändern oder indem Sie neue Daten in das Datenfeld eingeben.

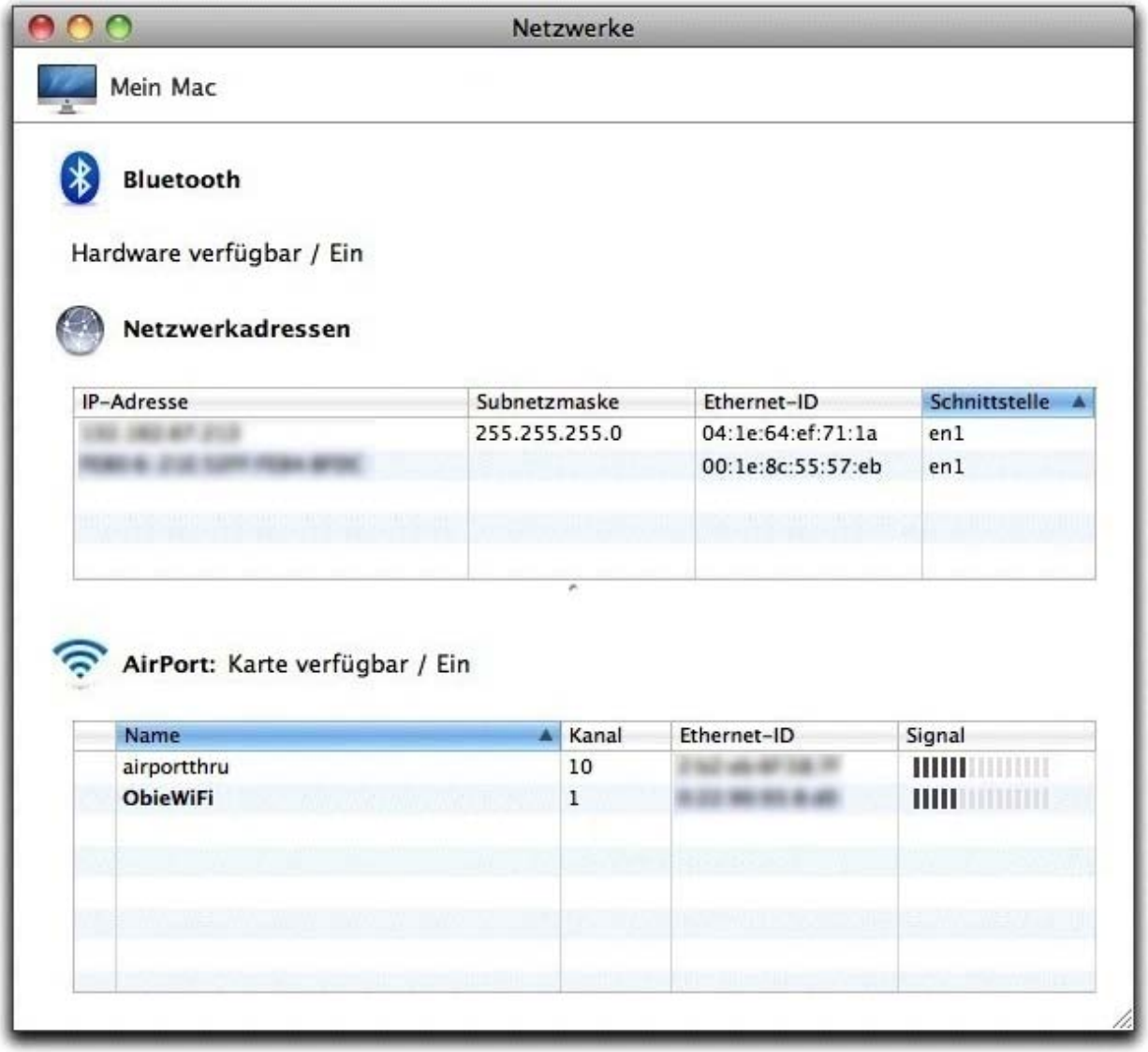
Wenn Sie Ihren Filter erstellt haben, klicken Sie zum Speichern auf "OK". Geben Sie dann in der Diensteliste einen Namen für den Filter ein. Klicken Sie jederzeit auf den Filter in der Liste, um sich die Netzwerkdienste anzeigen zu lassen, die mit Ihren Bedingungen übereinstimmten.

Ansehen der Netzwerkinformationen

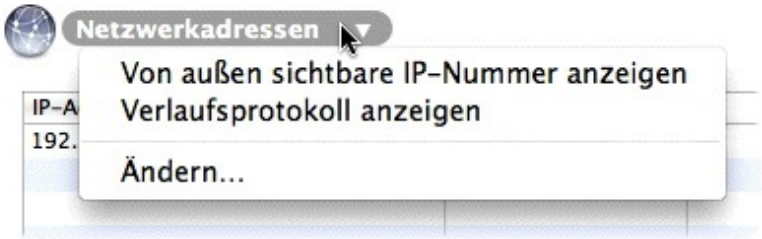
Das Netzwerkfenster zeigt hilfreiche Informationen über Ihren Mac an: die Netzwerkkonfiguration und die verfügbaren lokalen Netzwerke. Klicken Sie auf das Funkzeichen in der unteren rechten Ecke im Übersichtsfenster von VirusBarrier X6, um sich das Netzwerkfenster anzeigen zu lassen.

Das Netzwerkfenster zeigt Folgendes an:

- **Name Ihres Mac**: Wird in der grauen Leiste oben angezeigt: Im Beispiel unten ist das "Mein Mac". Das ist der Name, den Ihr Computer jedem anzeigt, der danach in einem Netzwerk sucht. Sie können diesen Namen im Fensterabschnitt "Sharing" der Systemeinstellungen ändern.
- **Bluetooth**: Zeigt an, ob Bluetooth-Hardware verfügbar und aktiv ist.
- **Netzwerkadressen**: Alle IP-Adressen, die auf Ihrem Mac aktiv sind. Wenn Sie mehrere Netzwerk-Adapter mit verschiedenen Adressen haben oder mehrere Server ausführen, wird mehr als eine Adresse angezeigt. Zeigt auch alle zugehörigen Subnetzmasken, Ethernet-IDs und Schnittstellen (im BSD-Namensformat) an.
- **AirPort**: Verfügbarkeit und Status einer kabellosen Netzwerkkarte. Wenn Ihre AirPort-Karte verfügbar und eingeschaltet ist, zeigt die Tabelle verfügbare kabellose Netzwerke, ihre Kanäle, Ethernet-IDs und Signalstärken für Ihren aktuellen Standort an. (Je dunkler die Balken, umso stärker ist das Signal.) Für kabellose Netzwerke, die ein Passwort erfordern oder einen anderen Schlüssel, wird ein kleines Schlosssymbol angezeigt. Für Netzwerke ohne Schloss benötigen Sie kein Passwort zum Aufbau einer Netzwerkverbindung. Sie können jedoch auf andere Weise geschützt sein, wie z.B. durch eine Web-Authentifizierung. Wenn Sie mit einem kabellosen Netzwerk verbunden sind, wird der Name in Fettdruck angezeigt.



Wenn Sie auf "Netzwerkadressen" klicken, stehen mehrere Funktionen und Optionen für das Netzwerkfenster zur Verfügung.



Zu diesen Optionen zählen:

- **Von außen sichtbare IP-Nummer anzeigen**: Diese Option zeigt in großer Schrift die IP-Adresse an, die Ihr Computer verwendet, wenn er mit dem Internet oder anderen Netzwerken verbunden wird. Diese IP-Nummer unterscheidet sich von der auf dieser Registerkarte angezeigten IP-Nummer, wenn Ihr Computer über einen Router oder ein Kabel oder ein DSL-Modem mit dem Internet verbunden ist. Klicken Sie auf eine beliebige Stelle auf dem Bildschirm, um die Information auszublenden.
- **Verlaufsprotokoll anzeigen**: Zeigt eine Liste mit den verschiedenen IP-Adressen an, die Ihrem Mac in der Vergangenheit von Ihrem ISP zugewiesen wurden. Dies ist jedoch nur zutreffend, wenn Ihrem Mac keine feste IP-Nummer zugewiesen wurde. Wenn Ihr Computer über einen Router, ein Kabelmodem oder ein DSL-Modem

mit dem Internet verbunden ist, wird lediglich die interne IP-Adresse Ihres Computers angezeigt.
- **Ändern...**: Öffnet das Netwerkfenster in den Systemeinstellungen von Mac OS X. Sie können in diesem Fensterabschnitt die Netzwerkeinstellungen für Ihren Computer ändern. Weitere Informationen über die Netzwerkeinstellungen erhalten Sie in der Hilfe zu Mac OS X.

Weitere Optionen stehen auch für einzelne Einträge im Abschnitt für Netzwerkadressen zur Verfügung. Sie können sich diese anzeigen lassen, indem Sie die Steuerungstaste gedrückt halten, während Sie auf den gewünschten Eintrag klicken. Daraufhin wird ein Kontextmenü geöffnet.

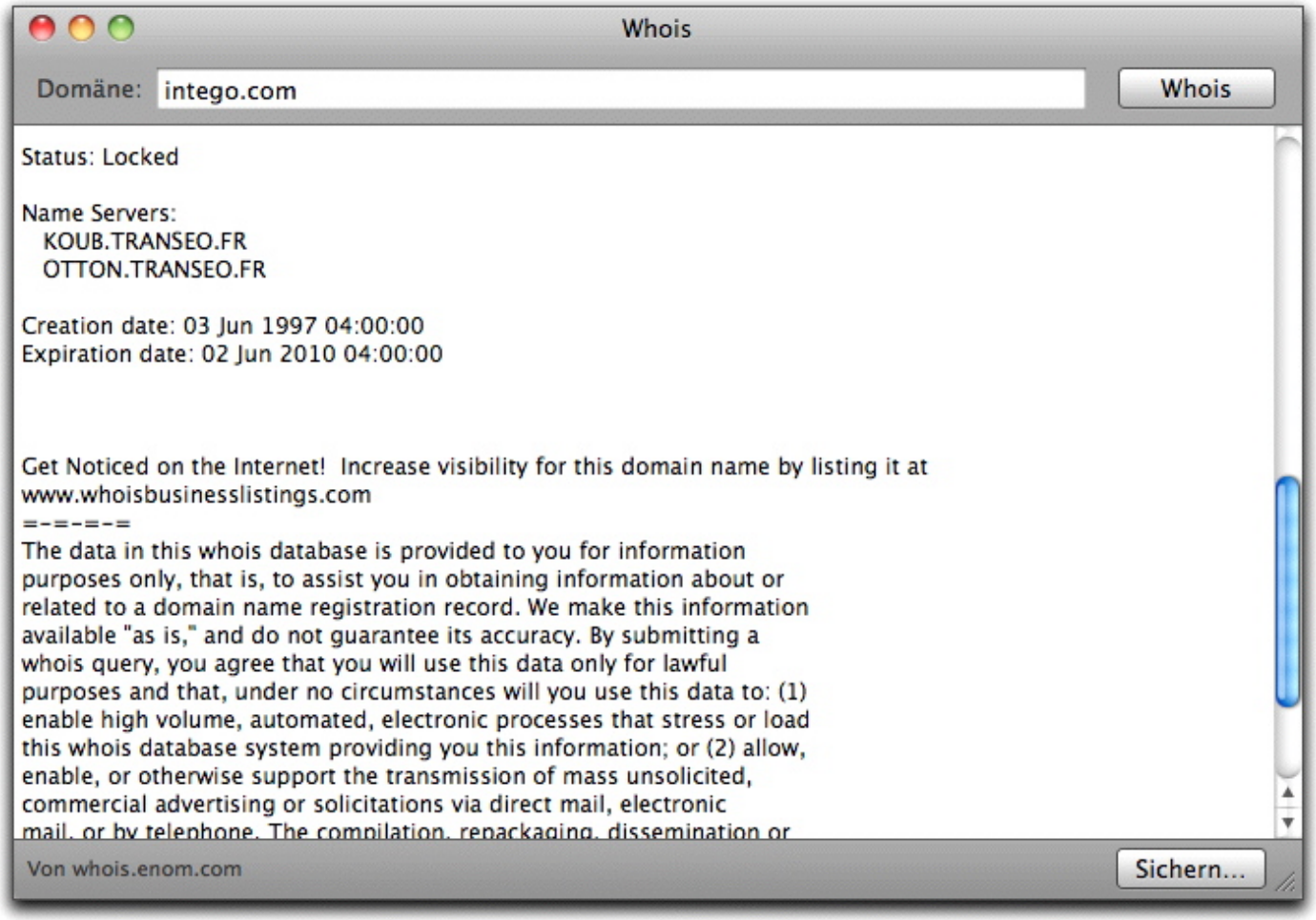
- **IP-Adresse in die Zwischenablage kopieren**: Kopiert die Informationen im Nur-Text-Format in die Zwischenablage von Mac OS X. Von dort aus können Sie diese in andere Programme einfügen.
- **Große Schrift**: Bietet die Möglichkeit, sich jede der drei Arten von Informationen für den Eintrag im Präsentationsmodus anzeigen zu lassen: die IP-Adresse, Subnetzmaske oder Ethernet-ID. Wenn Sie an eine beliebige Stelle auf dem Bildschirm klicken, wird die Anzeige in großer Schrift wieder ausgeblendet.

Wenn Sie schließlich mit der rechten Maustaste auf Einträge im AirPort-Abschnitt klicken, wird ein Kontextmenü geöffnet. Hier können Sie Ihren Mac von einem Netzwerk trennen, mit dem Sie derzeit verbunden sind.

Whois-Anfragen

In VirusBarrier X6 können Sie Domänennamen und Internet-IP-Adressen überprüfen, indem Sie die integrierte Whois-Funktion verwenden. Diese Funktion können Sie starten, indem Sie auf das Fragezeichensymbol in der unteren rechten Ecke des Bildschirms klicken.

Geben Sie dann einen Domänennamen oder eine IP-Nummer ins Domänenfeld ein und klicken Sie auf die Schaltfläche "Whois..." oder drücken Sie die Eingabetaste. Im Textfeld darunter sehen Sie nun die Informationen über die Domäne. Diese Informationen werden von öffentlich erreichbaren Informationsservern geliefert. Sie können diese Informationen in einer Textdatei sichern, indem Sie auf die Schaltfläche "Sichern..." klicken.


Whois
Domäne:
intego.com
Whois
Status: Locked
Name Servers:
KOUB.TRANSEO.FR
OTTON.TRANSEO.FR
Creation date: 03 Jun 1997 04:00:00
Expiration date: 02 Jun 2010 04:00:00
Get Noticed on the Internet! Increase visibility for this domain name by listing it at
www.whoisbusinesslistings.com
=-=-=-=
The data in this whois database is provided to you for information
purposes only, that is, to assist you in obtaining information about or
related to a domain name registration record. We make this information
available "as is," and do not guarantee its accuracy. By submitting a
whois query, you agree that you will use this data only for lawful
purposes and that, under no circumstances will you use this data to: (1)
enable high volume, automated, electronic processes that stress or load
this whois database system providing you this information; or (2) allow,
enable, or otherwise support the transmission of mass unsolicited,
commercial advertising or solicitations via direct mail, electronic
Von whois.enom.com
Sichern...

Nachdem Sie Ihre Informationen empfangen haben, zeigt der Text in dem grauen Balken am unteren Fensterrand Ihnen den Namen des Servers an, von dem die Informationen stammen. VirusBarrier X6 enthält standardmäßig vier Whois-Server. Sie können diese jedoch ändern oder weitere Whois-Server angeben. Weitere Informationen über das Hinzufügen von Whois-Servern finden Sie unter Einstellungen und Konfigurationen.

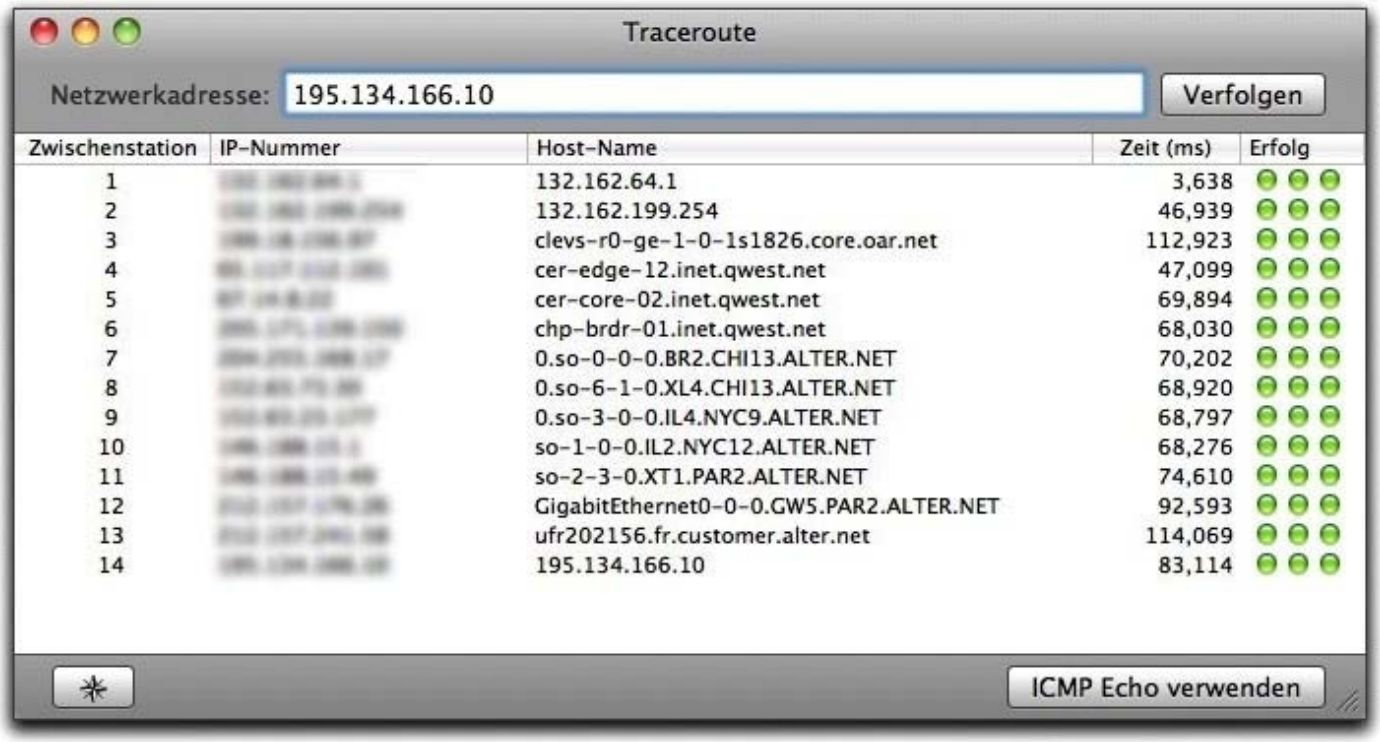
Traceroute-Suchen

Wenn Sie Daten ins Internet oder ein anderes Netzwerk senden oder von dort empfangen, werden die Daten in Paketen von einem Host zum anderen gesendet, bis sie das Datenziel erreichen. Auf diesem Weg machen sie Dutzende von Sprüngen. Mit der Traceroute-Funktion von VirusBarrier X6 können Sie genau verfolgen, wie Ihre Daten an ihr Ziel gelangen. Das ist vor allem dann hilfreich, wenn Sie Probleme haben, einen bestimmten Host zu erreichen und sehen möchten, wo die Daten blockiert werden. Wenn dies passiert bedeutet das normalerweise, dass ein Schlüssel-Host oder Router nicht funktioniert.

Starten Sie die Traceroute-Funktion von VirusBarrier X6, indem Sie auf die Schaltfläche mit dem "Y-Pfeil" in der unteren rechten Ecke des Bildschirms klicken.

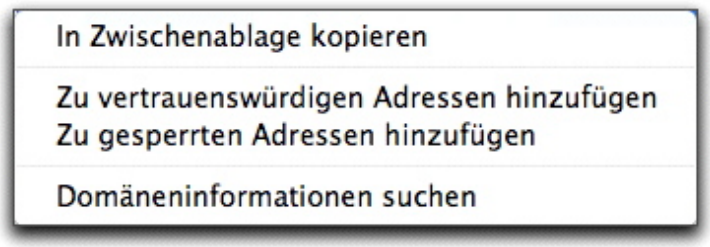
Sie können eine Traceroute-Suche ausführen, indem Sie eine IP-Adresse oder einen Domänennamen in das Feld "Netzwerkadresse" eingeben und dann auf die Schaltfläche "Verfolgen" klicken oder auf die Eingabetaste drücken. Wenn Sie einen Domänennamen eingeben, wird dieser von VirusBarrier X6 in die entsprechende IP-Adresse aufgelöst, die dann angezeigt wird. Wenn Sie auf "ICMP Echo verwenden" klicken, sendet Traceroute eine ICMP-Anfrage anstelle

einer UDP-Anfrage. In einigen Fällen kann das effektiver sein.



Im Fenster "Traceroute" werden nun alle Zwischenstationen (Relaisserver) zwischen Ihrem Computer und dem Zielserver angezeigt. Für jede Zwischenstation zeigt VirusBarrier X6 die laufende Nummer, die IP-Adresse, den Domänennamen, die Reaktionszeit in Millisekunden und die Anzahl der Ping-Datentelegramme an, die erfolgreich (grüne Kreise) oder nicht erfolgreich (rote Kreise) übertragen wurden. VirusBarrier X6 sendet für jede Zwischenstation oder jeden Schritt entlang der Route drei Pings. Wenn Ihr Computer über einen Router mit dem Internet verbunden ist, reagiert dieser unter Umständen nicht auf Ping-Anfragen. Hierdurch wird die Verfolgung der Ping-Datentelegramme bis zum gewünschten Zielserver jedoch nicht unmöglich gemacht.

Wenn Ihre Traceroute-Suche abgeschlossen ist, können Sie mit der rechten Maustaste auf einen Eintrag klicken, um sich das Kontextmenü anzeigen zu lassen.

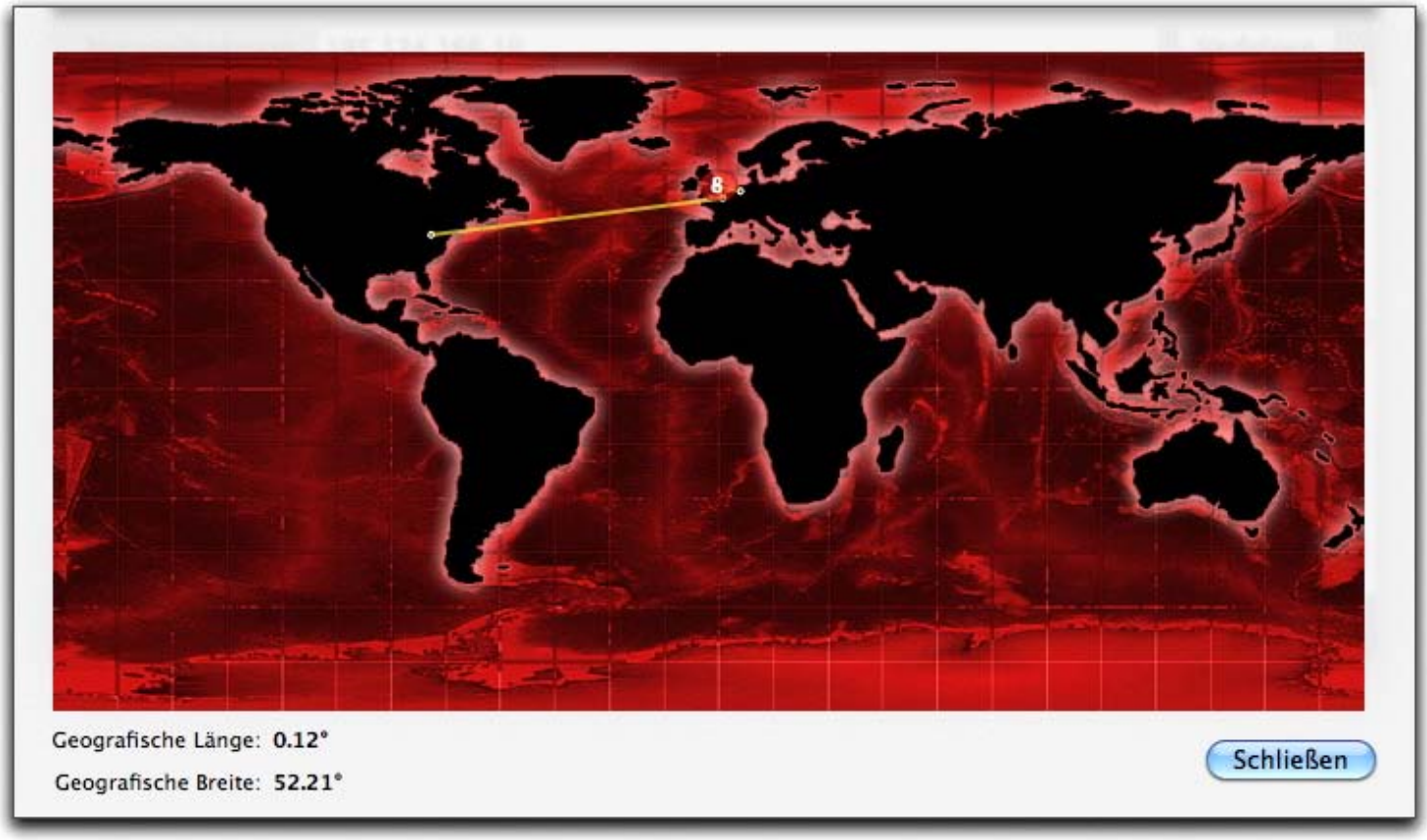


- **In Zwischenablage kopieren**: Kopiert die Informationen im Nur-Text-Format in die Zwischenablage von Mac OS X, damit Sie diese in andere Programme einfügen können.
- **Zu vertrauenswürdigen Adressen hinzufügen**: Fügt diese IP-Adresse dauerhaft der Liste mit vertrauenswürdigen Adressen hinzu. So werden künftige Datenübertragungen von dieser Adresse ungeachtet der Antivandalismus-Einstellungen erlaubt. Die Firewall von VirusBarrier X6 wird jedoch weiterhin auf die Datenübertragungen von dieser IP-Adresse angewendet.
- **Zu gesperrten Adressen hinzufügen**: Fügt diese IP-Adresse dauerhaft der Liste mit gesperrten Adressen hinzu. So werden künftige Datenübertragungen von dieser Adresse ungeachtet der Antivandalismus-Einstellungen unterbunden.
- **Domäneninformationen suchen**: Öffnet das Whois-Fenster von VirusBarrier X6 und führt eine Suche nach der

ausgewählten IP-Adresse durch.

Sie können eine visuelle Anzeige der Route sehen, die Ihre Daten zurücklegt, indem Sie auf das Windrosensymbol in der unteren linken Ecke klicken.

Auf der Weltkarte sehen Sie nun Linien, mit denen der Zielserver über die Zwischenstationen mit Ihrem Computer verbunden ist. Hierbei werden die Nummern aller beteiligten Computer angezeigt.



Wenn Sie auf die Google Earth-Schaltfläche in der unteren linken Ecke klicken und die Software Google Earth auf Ihrem Mac installiert haben, öffnet VirusBarrier X6 Google Earth und zoomt zu dem genauen geografischen Ort der IP-Adresse.

Beachten Sie bitte, dass dies nicht bei Adressen in Ihrem lokalen Netzwerk und auch nicht bei allen IP-Adressen funktioniert.

© 2009 Intego. Alle Rechte vorbehalten.

Einstellungen und Konfigurationen für VirusBarrier X6

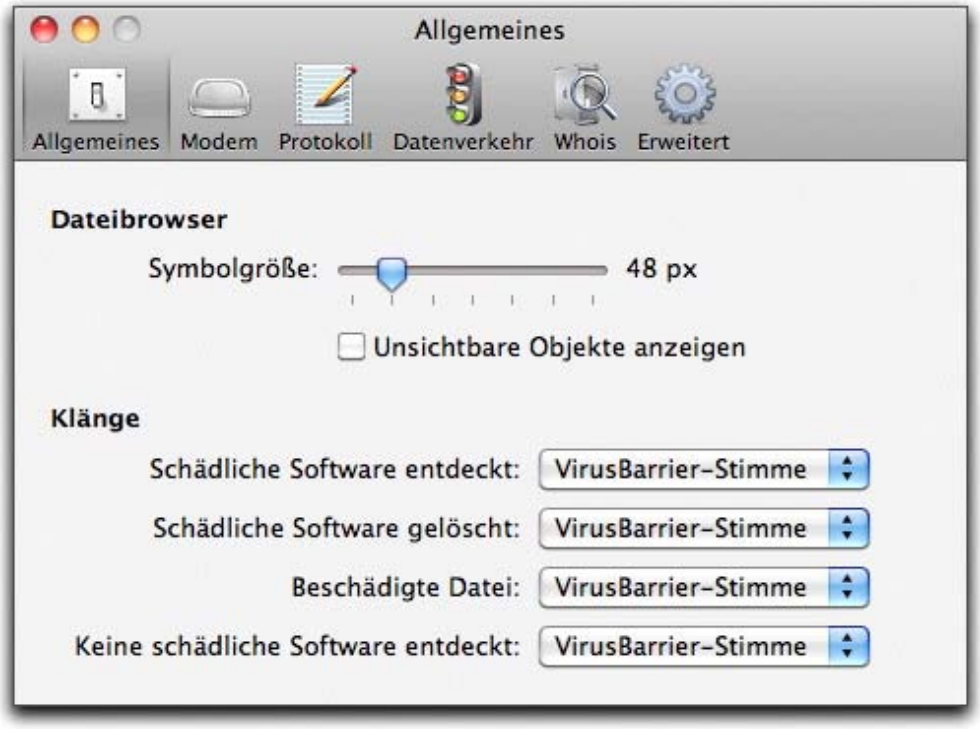
- Allgemeine Einstellungen
- Einstellungen für das Modem
- Einstellungen für das Protokoll
- Einstellungen für den Datenverkehr
- Einstellungen für Whois
- Erweiterte Einstellungen
- Arbeiten mit Konfigurationen

Zum Hauptinhaltsverzeichnis wechseln

VirusBarrier X6 wurde so entwickelt, dass es nach Installation diskret im Hintergrund arbeitet. Dennoch bietet es viele Optionen, mit denen Sie steuern können, wie die verschiedenen Funktionen ausgeführt werden und wie die Ergebnisse angezeigt werden, wenn Sie vorliegen. Sie können diese Optionen im Fenster "Einstellungen" einrichten. Wählen Sie "VirusBarrier X6 > Einstellungen..." oder drücken Sie Befehlstaste-Komma, um dieses Fenster zu öffnen.

Allgemeine Einstellungen

Das Einstellungsfenster ist in sechs Fensterabschnitte unterteilt: Allgemein, Modem, Protokoll, Datenverkehr, Whois und Erweitert.



Im oberen Abschnitt des Fensters für allgemeine Einstellungen können Sie festlegen, wie das Programm dargestellt werden soll. Im unteren Abschnitt legen Sie die Klänge fest. Es folgt eine Erklärung für jede Option.

Mit dem Schieberegler **Symbolgröße** können Sie festlegen, wie groß Symbole angezeigt werden sollen, wenn Sie im Übersichtsfenster auf "Auswählen" klicken, um Dateien und Ordner nach schädlicher Software zu durchsuchen und wenn Sie dabei die Symbolansicht verwenden. Außerdem legen Sie mit dem Schieberegler die Größe für Symbole fest, die in der Quarantänezone angezeigt werden. (Änderungen an dieser Einstellung haben keine Auswirkung, wenn Sie Objekte in der Listen- oder Spaltendarstellung anzeigen.)

Mit der zweiten Option, **Unsichtbare Objekte anzeigen** können Sie sich Dateien anzeigen lassen, die von Mac OS X normalerweise ausgeblendet werden. Dies sind normalerweise Dateien, die benötigt werden, damit der Mac ordnungsgemäß funktioniert. Diese Dateien sollten nicht geändert werden. Viren und schädliche Software können sich in unsichtbaren Dateien verstecken. Deshalb ist es sehr wichtig, dass diese Dateien gescannt werden. Sie müssen sich diese Dateien jedoch nicht anzeigen lassen, um sie nach schädlicher Software zu durchsuchen: Wenn Sie einen Ordner nach schädlicher Software durchsuchen, scannt VirusBarrier X6 jedes darin befindliche Element, einschließlich der unsichtbaren Elemente.

Beachten Sie, dass in der Quarantänezone immer unsichtbare Objekte angezeigt werden, unabhängig davon, was in den Einstellungen festgelegt wurde.

Im Bereich "Klänge" können Sie festlegen, was Sie hören, wenn VirusBarrier X6 schädliche Software entdeckt oder entfernt, eine beschädigte Datei findet oder wenn das Programm einen Scanvorgang beendet, ohne schädliche Software gefunden zu haben. Standardmäßig ist eingestellt, dass diese Hinweise gesprochen werden: Sie können sich anhören, wie das klingt, indem Sie auf das entsprechende Popup-Menü klicken und noch einmal "VirusBarrier-Stimme" auswählen. Sie können jeden Klang auch ändern, indem Sie in diesem Popup-Menü einen anderen Klang auswählen. Wenn Sie einen der Klänge ganz ausschalten möchten, wählen Sie aus dem entsprechenden Popup-Menü "Keine" aus.

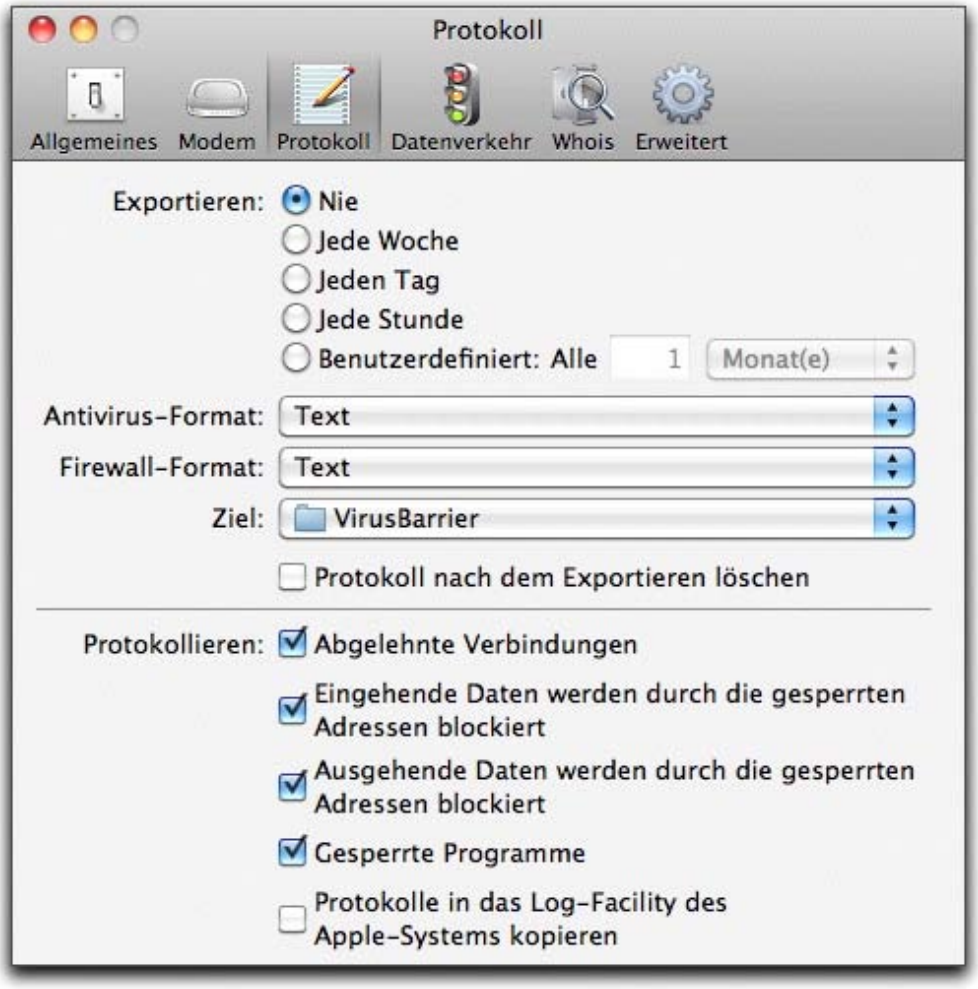
Einstellungen für das Modem

Mit dieser Option können Sie Ihr Modem so konfigurieren, dass es keine Anrufe annehmen kann. Klicken Sie hierzu im

Einstellungsfenster auf die Schaltfläche "Modem". Wenn Sie Ihr Modem sichern, kann es keine Anrufe mehr entgegennehmen. Wenn Sie auf die Schaltfläche "Jetzt schützen" klicken, wird VirusBarrier X6 keine eingehenden Anrufe akzeptieren: Sie können jedoch weiterhin ausgehende Anrufe tätigen. Durch Klicken auf die Schaltfläche "Zurücksetzen" können Sie Ihr Modem wieder in den normalen, ungesicherten Zustand zurücksetzen.

Einstellungen für das Protokoll

Sie können VirusBarrier X6 so konfigurieren, dass das Protokoll automatisch in von Ihnen vorgegebenen Zeitintervallen exportiert wird. Klicken Sie hierzu im Einstellungsfenster auf die Schaltfläche "Protokoll".



Wählen Sie zuerst, wie oft das Protokoll exportiert werden soll. Wenn das runde Optionsfeld "Jede Woche" markiert ist, wird das Protokoll immer um Mitternacht, von Sonntag auf Montag exportiert. Wenn "Jeden Tag" markiert ist, wird es täglich um Mitternacht exportiert. Wenn "Jede Stunde" markiert ist, wird es zu jeder vollen Stunde exportiert. Sie können auch eine benutzerdefinierte Option wählen und mehrere dieser Zeitpunkte eingeben, beispielsweise einmal alle zwei Wochen. (Mit der benutzerdefinierten Option können Sie das Protokoll auch einmal im Monat exportieren lassen, um Mitternacht des ersten Tages.)

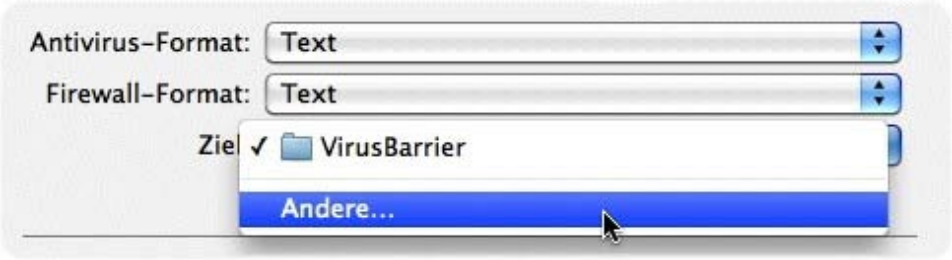
Wenn Ihr Mac zum Zeitpunkt des geplanten Exportvorgangs ausgeschaltet ist, wird das Protokoll dann exportiert, wenn Sie ihn das nächste Mal wieder einschalten.

Antivirus-Protokolle können in drei Formaten exportiert werden, Firewall-Protokolle in sechs Formaten. Klicken Sie auf das Popup-Menü "Format", um das Exportformat zu wählen.

Hinweis: Eine Beschreibung der Protokollexportformate erhalten Sie weiter hinten in diesem Kapitel unter "So exportieren Sie das Protokoll".

Sie können den Ordner wählen, in dem die Protokolldateien gespeichert werden sollen. Standardmäßig wird die Datei

im Ordner /Library/Logs/VirusBarrier gespeichert. Wenn diese Dateien in einem anderen Ordner gespeichert werden sollen, müssen Sie auf die Schaltfläche "Andere..." im Popup-Menü klicken und zum gewünschten Ordner navigieren. Klicken Sie dann auf die Schaltfläche "Wählen", um diesen Ordner als Speicherort zu verwenden.



VirusBarrier X6 speichert zwei Netzwerk-Protokolle. Es gibt ein Umlaufprotokoll, das höchstens 4096 Einträge enthält, die Ihnen im Protokollpaneel von VirusBarrier X6 angezeigt werden. Wenn das automatische Exportieren aktiviert ist, werden alle Einträge in einem zweiten Protokoll gespeichert. Wenn Sie vollständige Protokolle aller Aktivitäten aufbewahren möchten, sollten Sie regelmäßige Exporte aktivieren. Diese Protokolle werden nicht durch die Größe begrenzt (außer durch den verfügbaren freien Speicherplatz auf Ihrer Festplatte). Wenn Sie die Option "Protokoll nach dem Exportieren löschen" wählen, werden nach jedem Exportvorgang die Protokolleinträge gelöscht. So enthält jede neue Exportdatei nur die Einträge, die im Anschluss an den vorigen Export aufgezeichnet wurden. Diese Einstellung hat nur Auswirkungen auf automatisierte Exportvorgänge und nicht auf das manuelle Exportieren von Protokollen aus dem Protokollfenster.

Sie können auswählen, welche Elemente in Ihren Protokollen gespeichert werden sollen - wie durch die Kontrollkästchen am unteren Rand des Einstellungsfensters für Protokolle angezeigt. Sie haben folgende Optionen:

- **Abgelehnte Verbindungen**: Versuche auf Ihren Mac zuzugreifen, die gesperrt wurden, weil von Ihnen in VirusBarrier X6 eingestellte Regeln verletzt wurden.
- **Eingehende Daten von gesperrten Adressen**: Versuche von Hosts, die auf Ihrer Liste mit gesperrten Adressen stehen, Daten an Ihren Mac zu senden.
- **Ausgehende Daten an gesperrte Adressen**: Versuche Daten von Ihrem Mac an Hosts zu senden, die auf Ihrer Liste mit gesperrten Adressen stehen.
- **Gesperrte Programme**: Fälle in denen die Anti-Spyware von VirusBarrier X6 dafür gesorgt hat, dass ein Programm keine Datenverbindung zu einem Netzwerk aufbaut.

Das letzte Kontrollkästchen lautet "Protokolle in Apples Log-Facility kopieren". Wenn dieses Kontrollkästchen markiert ist, werden die Protokolldaten in dem gemeinsamen Protokollsystem von Mac OS X 10.5 und neuer gespeichert. Sie können Sie diese Protokolle im Programm "Konsole" ansehen, das sich im Ordner "/Programme/Dienstprogramme" befindet.

Einstellungen für den Datenverkehr

Wie bei den Einstellungen für das Protokoll können Sie auch im Einstellungsfenster für den Datenverkehr zwischen verschiedenen Option für das Exportieren von Daten in regelmäßigen Zeitabständen wählen. Im nun geöffneten Fenster können Sie festlegen, wann und wie die Datenverkehrsdaten exportiert und verwaltet werden sollen. Klicken Sie zum Ändern der Einstellungen auf die Schaltfläche "Datenverkehr" im Einstellungsfenster.

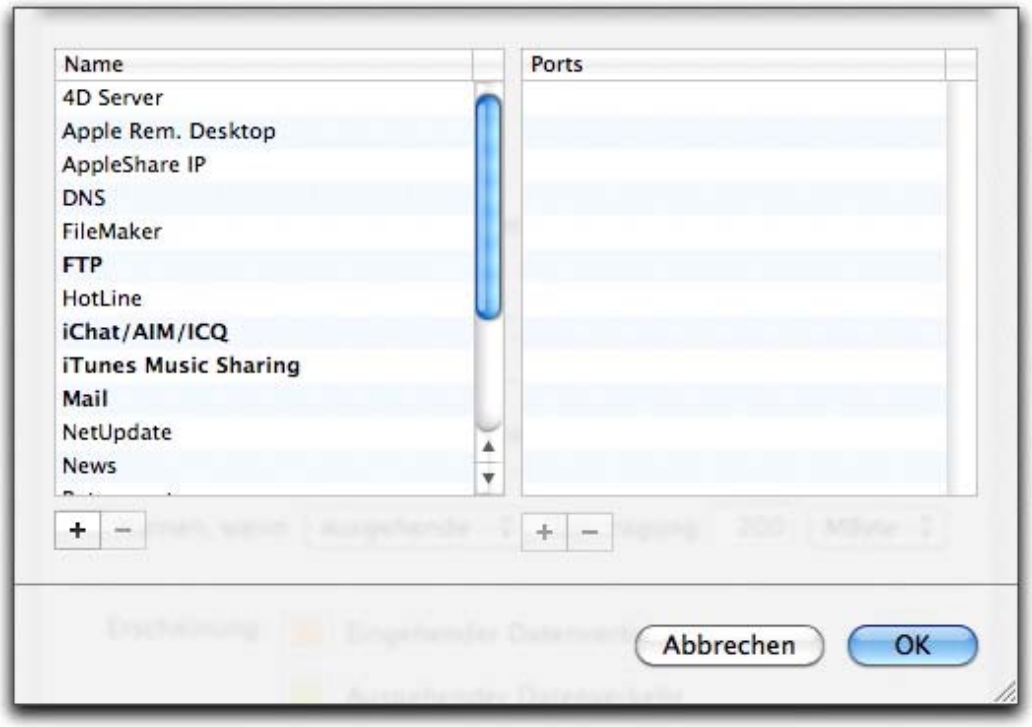
Im oberen Fensterabschnitt können Sie automatisierte, regelmäßige Exportvorgänge für den Datenverkehr festlegen. Das funktioniert genau so, wie bei den Einstellungen für das Protokoll. Weitere Informationen finden Sie im Abschnitt über die Einstellungen für das Protokoll weiter vorn. Es gibt jedoch eine Einstellung, die sich von den vorherigen unterscheidet: das Kontrollkästchen "Anzeigepegel nach dem Exportieren zurücksetzen". Dabei handelt es sich im Prinzip um die gleiche Funktion wie "Protokoll nach dem Exportieren löschen". Wenn Sie das Kontrollkästchen markieren, passiert das Gleiche wie wenn Sie auf die Schaltfläche zum Zurücksetzen neben den Anzeigepegeln klicken, um den Gesamtdatenverkehr nach den automatisierten Exportvorgängen auf Null zurückzusetzen. Weitere Informationen über die Anzeigepegel für den Datenverkehr finden Sie unter So verwenden Sie die Überwachungstools von VirusBarrier X6.

In den Einstellungen für den Datenverkehr von VirusBarrier X6 gibt es auch eine Option, die Sie darüber informiert, wenn die Anzahl der auf Ihrem Computer ein- oder ausgehenden Daten eine bestimmte Grenze überschreitet. Diese Funktion ist sehr nützlich, wenn das Datenverkehrsaufkommen (Datenvolumen, Datenmenge) Ihres Internet-Zugangs für gesendete und/oder empfangene Daten begrenzt ist.

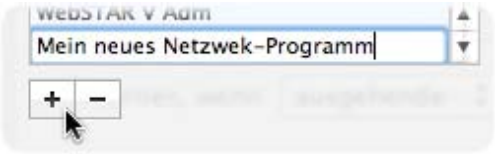
Wenn Sie diese Option markiert haben, gibt VirusBarrier X6 eine Warnmeldung aus, sobald das Datenverkehrsaufkommen Ihres Computers den vorgegebenen Grenzwert überschritten hat. Sie können festlegen, ob eine Warnmeldung bei ein- und/oder ausgehendem und/oder für den gesamten Datenverkehr ausgegeben soll. Zudem können Sie den Grenzwert in Kilobyte, Megabyte oder Gigabyte angeben.

Darunter gibt es einen Abschnitt für die Darstellung. Hier können Sie die Farbe für den ein- und ausgehenden Datenverkehr in allen Anzeigepegeln und Zeitachsen für den Datenverkehr ändern. Wenn Sie auf eines der farbigen Kästchen klicken, wird die Standard-Farbauswahl von Mac OS X geöffnet: Wählen Sie die gewünschte Farbe aus und schließen Sie das Fenster dann, indem Sie auf das rote Schließsymbol in der oberen linken Ecke klicken. Wenn Sie auf die Schaltfläche "Auf Standardeinstellungen zurücksetzen" klicken, wird der eingehenden Datenverkehr wieder orange und der ausgehende Datenverkehr grün angezeigt.

Schließlich gibt es noch eine Schaltfläche für Dienste im unteren Abschnitt, mit der Sie die Art des in den Anzeigepegeln dargestellten Datenverkehrs verändern können. Diese Option ist sehr hilfreich, wenn Sie ein neues Netzwerkprogramm ausprobieren. Wenn Sie auf die Schaltfläche "Liste bearbeiten..." klicken, wird ein Fenster geöffnet, in dem die vorhandenen Dienste aufgeführt sind.



Wenn Sie einen Dienst hinzufügen möchten, klicken Sie auf die Schaltfläche "+" in der unteren linken Ecke des Fensters und geben Sie dann den Namen des Dienstes ein.



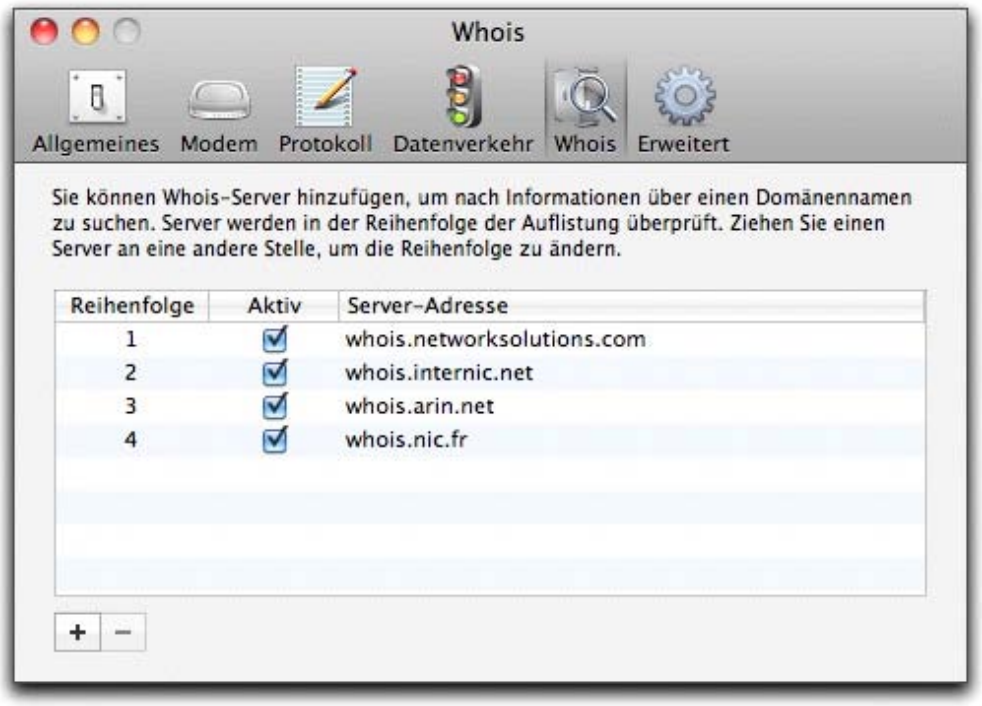
Wenn Sie dann auf das andere Pluszeichen unter der rechten Spalte klicken, solange der Dienst markiert ist, können Sie die zu diesem Programm zugehörigen Ports hinzufügen.

In ähnlicher Weise können Sie alle Dienste in der Liste bearbeiten oder löschen, die nicht in Fettdruck aufgeführt sind. Die fettgedruckten Dienste, wie beispielsweise Chat, Mail und Web, zählen zum Kern der Arbeit mit Netzwerken und sind daher aus Sicherheitsgründen für Veränderungen gesperrt.

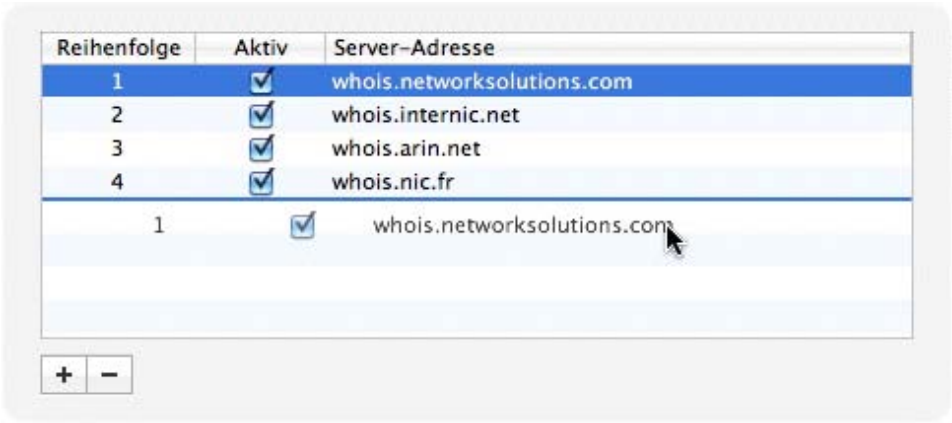
Einstellungen für Whois

Mit der Whois-Funktion von VirusBarrier X6 können Sie den Domänennamen oder die IP-Adresse suchen lassen. In

diesem Dialogfeld sind bereits vier Whois-Server vordefiniert, die in der angezeigten Reihenfolge abgefragt werden.



Sie können die Reihenfolge der Abfrage ändern, indem Sie auf den Domänennamen des betreffenden Whois-Servers klicken und diesen dann an die gewünschte Position ziehen.



Das Hinzufügen neuer Whois-Server zu VirusBarrier X6 ist ganz einfach: Klicken Sie einfach auf das Pluszeichen (+) und geben Sie den Namen des neuen Whois-Servers ein.

Sie können die Whois-Server in diesem Fenster auch aktivieren oder abschalten. Wenn Sie einen Server abschalten wollen, müssen Sie in das Kontrollkästchen links vom Namen des Filters klicken, sodass dort kein Häkchen erscheint. Um einen abgeschalteten Whois-Server wieder zu aktivieren, müssen Sie das entsprechende Kontrollkästchen markieren.

Wenn Sie einen Whois-Server entfernen möchten, klicken Sie zur Auswahl auf den entsprechenden Server und anschließend auf die Schaltfläche "-". In einem Dialogfeld werden Sie dann gebeten, den Vorgang zu bestätigen.

Erweiterte Einstellungen

Im Fensterabschnitt "Erweitert" in den Voreinstellungen für VirusBarrier X6 stehen Ihnen vier Optionen zur Auswahl.

- **Schutz**: Dabei handelt es sich um einen einfachen Ein-/Aus-Schieberegler, mit dem Sie *alle* Schutzfunktionen von VirusBarrier X6 schnell ein- oder ausschalten können. Wenn Sie diesen Schieberegler auf "Aus" stellen, wird VirusBarrier X6 komplett abgeschaltet, einschließlich der Firewall-Protokollierung. Hierzu benötigen Sie ein Administrator-Passwort - ebenso, um den Schieberegler wieder auf "Ein" zu stellen. Ungeachtet dieser Einstellung wird VirusBarrier X6 automatisch wieder aktiviert, wenn Sie Ihren Mac neu starten.
- **Konfiguration**: Wenn Sie auf die Schaltfläche "Zur Standardeinstellung zurückkehren..." klicken, wird VirusBarrier X6 auf die Standard-Konfiguration zurückgesetzt: Client, lokaler Server-Modus für die Firewall und die Antivandalismus- sowie Datenschutzfunktionen sind deaktiviert. Für den Schutz vor schädlicher Software aktivieren diese Einstellungen den Echtzeit-Scanner, deaktivieren das Scannen von Archiven und aktivieren bestimmte erweiterte Scanner-Einstellungen. Für diese Änderung benötigen Sie ein Administratorkennwort. Durch diesen Vorgang werden alle Firewall-Modi und alle anderen von Ihnen vorgenommenen Einstellungen ebenso wie Ihre Liste mit gesperrten Adressen und Ihre Liste mit vertrauenswürdigen Adressen gelöscht. Wir empfehlen Ihnen, Ihre aktuellen Einstellungen für VirusBarrier X6 zu exportieren (Ablage > Einstellungen exportieren...), bevor Sie zu den Standardeinstellungen zurückkehren, falls Sie Ihre Einstellungen später erneut verwenden möchten.
- **Konfigurationsassistent**: Wenn Sie auf die Schaltfläche "Assistenten anzeigen..." klicken, wird der Konfigurationsassistent von VirusBarrier X6 gestartet. Weitere Informationen erhalten Sie unter Erste Schritte mit Intego VirusBarrier X6.

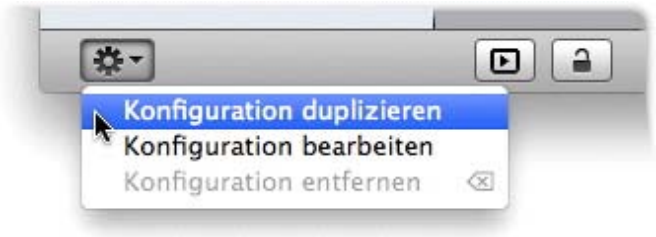
Arbeiten mit Konfigurationen

Sie können mehrere Konfigurationen für VirusBarrier X6 speichern. Jede Konfiguration enthält alle Einstellungen, die Sie in den verschiedenen Fenstern und Einstellungen von VirusBarrier X6 festgelegt haben. Sie können Konfigurationen für verschiedene Orte definieren. Beispielsweise eine Konfiguration dafür, wenn Sie Ihr Laptop im Büro verwenden und eine andere dafür, wenn Sie es zuhause verwenden. Unter Umständen wollen Sie eine Konfiguration mit zusätzlichem Schutz verwenden, wenn Sie Ihren Mac als Server einsetzen, während eine andere Konfiguration verwendet wird, wenn Ihr Mac nur als Client arbeitet. Sie können beispielsweise auch eine eigene Konfiguration speichern, die Sie verwenden, wenn Ihr Computer mit einem lokalen Netzwerk verbunden ist. Eine andere Konfiguration bietet zusätzlichen Schutz, wenn Sie öffentliche Hotspots nutzen. Eventuell sollten Sie eine Konfiguration definieren, in der Sie festgelegt haben, dass das Programm Ihnen eine E-Mail schicken soll, sobald ein Eindringversuch erkannt wurde, wenn Sie nicht in der Nähe Ihres Computers sind.

Konfigurationen werden immer in einer Liste in der linken Fensterhälfte angezeigt. Mit einer kleinen Aktionsschaltfläche unterhalb der Liste können Sie die Konfigurationen duplizieren, bearbeiten, entfernen oder ausblenden. Wenn die Konfigurationsliste nicht angezeigt wird, ist sie vielleicht ausgeblendet: Sie können die Konfigurationsliste einblenden, indem Sie "Wahltaste-K" drücken, "Ansicht > Konfigurationen anzeigen" wählen oder indem Sie auf die Schaltfläche "Konfigurationen ein/aus" in der unteren linken Ecke des Fensters klicken.

Erstellen, Bearbeiten und Löschen von Konfigurationen

Wenn Sie VirusBarrier X6 das erste Mal verwenden, wird eine Konfiguration in der Liste angezeigt. Sie trägt den Namen, den Sie im Konfigurationsassistenten für die Konfiguration gewählt haben. Wenn Sie den Konfigurationsassistenten nicht ausgeführt haben, heißt sie "Standard". Wenn Sie eine neue Konfiguration erstellen möchten, duplizieren Sie eine vorhandene Konfiguration, indem Sie sie zuerst markieren und dann auf die Aktionsschaltfläche klicken und diese gedrückt halten (die Schaltfläche sieht aus wie ein Zahnrad). Wählen Sie dann "Konfiguration duplizieren".



Diese neue Konfiguration trägt den gleichen Namen, wie die von Ihnen duplizierte Konfiguration, an den das Wort "Kopie" angehängt wird. Geben Sie der neuen Konfiguration einen neuen Namen, indem Sie darauf doppelklicken und einen neuen Namen eingeben.

Jetzt können Sie die neue Konfiguration aktivieren, indem Sie auf das zugehörige runde Optionsfeld klicken. In unserem Beispiel haben wir zwei neue Konfigurationen erstellt, indem wir die Standard-Konfiguration zwei Mal dupliziert haben. Dann haben wir sie umbenannt und die ausgewählt, die jetzt "Privat" heißt.

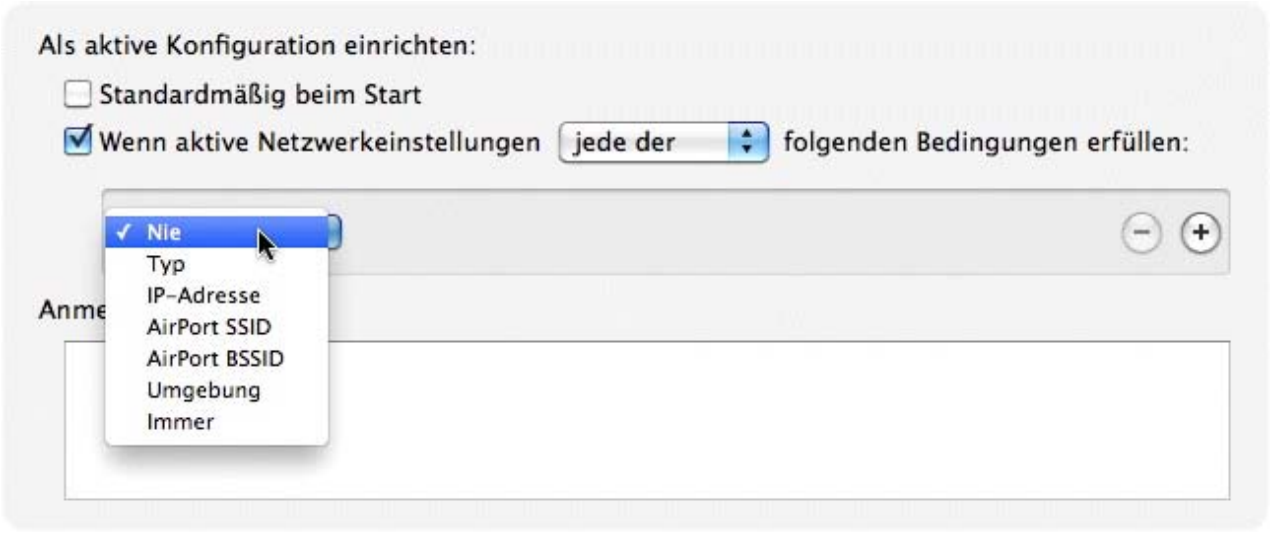
Sie können jetzt die von Ihnen gewünschten Änderungen an VirusBarrier X6 vornehmen, die dann in der aktuellen Konfiguration gespeichert werden. Wenn Sie eine andere Konfiguration aktivieren möchten, klicken Sie einfach auf das entsprechende runde Optionsfeld. Sie können eine andere Konfiguration auch aus der Konfigurationsliste im Intego-Menü auswählen. (Weitere Informationen über das Intego-Menü erhalten sie unter Erste Schritte mit Intego VirusBarrier X6.)

Sobald Sie die Konfiguration erstellt haben, können Sie diese bearbeiten, indem Sie auf die Aktionsschaltfläche unterhalb der Konfigurationsliste klicken und "Konfiguration bearbeiten" auswählen. Ihnen wird dann ein Fenster wie

dieses angezeigt:

Diese Konfiguration wird aktiviert, wenn Sie Ihren Mac einschalten oder neu starten, wenn Sie das Kontrollkästchen "Standardmäßig beim Start" markiert haben.

Zudem wird die Konfiguration automatisch aktiviert, wenn Sie das Kontrollkästchen "Wenn aktive Netzwerkeinstellungen..." markieren und wenn eine oder alle von Ihnen für die folgenden Netzwerkkriterien festgelegten Bedingungen eintreten.



- **Nie**: Diese Bedingung tritt nie ein, daher wird die Konfiguration auch niemals automatisch eingeschaltet.
- **Typ**: Sie können wählen zwischen Ethernet, AirPort, FireWire, PPP oder Bluetooth.
- **IP-Adresse**: Sie können eine bestimmte IP-Adresse wählen oder einen Bereich. Die Schaltfläche "Aktuell" zeigt an, welche IP-Adresse Ihr Mac gerade verwendet.
- **AirPort SSID**: Der übliche Name für ein kabelloses Netzwerk, z.B. "Mein AirPort". Sie können auswählen, dass

diese Bedingung eintreten soll, wenn die SSID entweder mit einer von Ihnen festgelegten Zeichenfolge übereinstimmt, nicht übereinstimmt oder Teile davon enthält.
- **AirPort BSSID**: Die MAC-Adresse eines kabellosen Netzwerk-Verbindungspunkts. Sie wird als Zeichenfolge in Hexadezimal-Ziffern angegeben.
- **Speicherort**: Der in den Netzwerkeinstellungen Ihres Mac festgelegte Speicherort.
- **Immer**: Die Bedingung trifft immer zu.

Im Anmerkungsfeld können Sie eine Beschreibung oder Notizen eingeben, die Sie hinzufügen möchten. Sie haben keinerlei Auswirkungen auf die Funktionsweise der Konfiguration.

Sie können die Konfiguration auf zwei Arten löschen. Klicken Sie zuerst ein Mal auf die Konfiguration. Dann können Sie entweder auf die Aktionsschaltfläche unterhalb der Konfigurationsliste klicken und "Konfiguration entfernen" auswählen oder Sie drücken "Wahltaste-Löschtaste". In beiden Fällen wird daraufhin ein Dialogfeld angezeigt, in dem Sie den Löschvorgang bestätigen müssen. Sie können die aktive Konfiguration nicht entfernen. Wechseln Sie stattdessen in eine andere Konfiguration, bevor Sie diese löschen.

Exportieren und Importieren von Einstellungen

Sie können Ihre Einstellungen von VirusBarrier X6 in einer Datei speichern, aus der Sie die Einstellungen auf einem anderen Computer mit installiertem VirusBarrier X6 importieren können. Dies ist vor allem dann hilfreich, wenn Sie mehrere Computer verwalten und für alle Computer die gleichen Einstellungen verwenden wollen.

Wählen Sie zum Exportieren der Einstellungen "Ablage > Einstellungen exportieren..." aus. Daraufhin werden Sie in einem Dialogfeld aufgefordert, einen Namen für die Datei mit den Einstellungen einzugeben und einen Speicherort zu wählen. Klicken Sie auf "Exportieren", wenn Sie fertig sind. Sie erhalten dann eine XML-Datei, die Sie in jede Kopie von VirusBarrier X6 importieren können. Auch in die, in der die Datei erstellt wurde.

Wählen Sie hierzu die Option "Ablage > Einstellungen importieren…". In einem Dialogfeld werden Sie aufgefordert, die Datei mit den Einstellungen zu suchen. Wenn Sie die Datei gefunden haben, klicken Sie auf "Importieren". Diese Einstellungen werden dann sofort auf VirusBarrier X6 angewendet. Sie können auch auf die Einstellungsdatei von VirusBarrier X6 doppelklicken, um sie zu importieren.

© 2009 Intego. Alle Rechte vorbehalten.

So erstellen Sie eigene Firewall-Regeln

- Eigene Firewall-Regeln
- So erstellen Sie Regeln mit dem Assistenten
- So erstellen Sie Dienste-spezifische Regeln schnell
- So erstellen Sie Regeln manuell
- Arbeiten mit Regeln

Zum Hauptinhaltsverzeichnis wechseln

Eigene Firewall-Regeln

Jede der in Kapitel 4 (So schützen Sie Ihren Mac vor Netzwerk-Angriffen) beschriebenen fünf Firewall- Einstellungen ist in Wirklichkeit eine Sammlung von Regeln, von denen jede durch das Benennen von erlaubten und verbotenen Quellen, Zielen, Diensten und Schnittstellen definiert wird.

Im einfachen Modus dürfen Sie die Regeln oder Teile davon nicht verändern. Hierzu müssen Sie in den erweiterten Modus im Firewall-Fenster wechseln. Klicken Sie hierzu auf die Schaltfläche "Firewall" am oberen Rand des Hauptfensters.

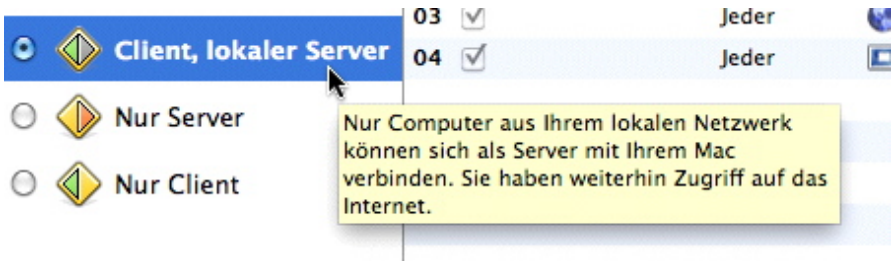
Klicken Sie dann auf die Registerkarte "Firewall-Regeln", wenn sie noch nicht aktiv ist, und auf die Schaltfläche "Erweiterter Modus" in der oberen rechten Ecke.

ACHTUNG: Das Ändern dieser Einstellungen kann schwerwiegende Auswirkungen auf die Fähigkeit Ihres Computers haben, auf lokale Netzwerke und das Internet zuzugreifen. Sie sollten den erweiterten Modus nur verwenden, wenn Sie die Auswirkungen und die Funktionsweise wirklich verstehen.

Im einfachen Modus wird eine Animation angezeigt, wenn Sie auf die fünf voreingestellten Firewall-Konfigurationen

klicken. Im erweiterten Modus werden Ihnen die Einzelheiten der Regeln für jede einzelne Einstellung angezeigt.

Zudem wird ein Text mit einer kurzen Beschreibung der Auswirkungen der jeweiligen Einstellung angezeigt, wenn Sie einige Sekunden mit dem Mauszeiger darüber fahren.


Client, lokaler Server
Nur Server
Nur Client
03 Jeder
04 Jeder
Nur Computer aus Ihrem lokalen Netzwerk können sich als Server mit Ihrem Mac verbinden. Sie haben weiterhin Zugriff auf das Internet.

In diesem Beispiel hat die Einstellung "Client, lokaler Server" vier Regeln. Die erste erlaubt dem lokalen Netzwerk den Zugriff auf Ihren Mac über alle verbundenen Dienste. Das sind TCP-Verbindungen, die mit einer Kommunikation in beide Richtungen verbunden sind, wie beispielsweise das zur Verfügung stellen von Dateien von Ihrem Mac. Die zweite Regel jedoch verbietet solche Verbindungen über das Internet und lässt Ihren Mac somit nicht als Server für einen unbekannten Computer außerhalb Ihres lokalen Netzwerks dienen. Die dritte Regel erlaubt alle anderen Kommunikationsarten aus dem Internet mit Ihrem Mac und die vierte erlaubt alle Kommunikationsarten von Ihrem Mac *zum* Internet.

Die fünf voreingestellten Firewall-Einstellungen werden "eingefroren", damit Sie praktisch und stabil sind: Sie können die Regeln oder die Reihenfolge, in der sie erscheinen, nicht ändern. VirusBarrier X6 bietet Ihnen jedoch zwei Möglichkeiten, um zusätzliche, eigene Einstellungen zu erstellen: über den Firewall-Assistenten des Programms und manuell.

In jedem Fall müssen Sie zuerst auf die Schaltfläche "+" unter der Liste mit den Einstellungen klicken. Daraufhin wird eine neue Einstellung namens "unbenannte Einstellungen" angezeigt. Klicken Sie darauf und geben Sie einen beliebigen Namen ein. Drücken Sie dann auf die Eingabetaste, um die Änderung dauerhaft zu akzeptieren.

Denken Sie bitte daran, dass Sie die Einstellung jetzt nur erstellt haben, Sie haben sie aber noch **nicht** aktiviert. Am besten aktivieren Sie die Firewall-Einstellungen erst, wenn Sie alle Ihre Regeln hinzugefügt haben. Klicken Sie zum Aktivieren der Einstellung auf das runde Optionsfeld links neben der entsprechenden Einstellung.

So erstellen Sie Regeln mit dem Assistenten

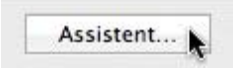
VirusBarrier X6 enthält einen Assistenten, der Sie dabei unterstützt, Ihre eigenen Firewall-Regeln zu definieren. Dank diesem Assistenten brauchen Sie hierfür nur wenige Mausklicks. Mit dem Regelassistenten können Sie zwar nicht auf alle Regeln von VirusBarrier X6 zugreifen, doch decken die damit definierbaren Regeln die meisten Anwendungsfälle

ab. Wenn Sie eine weitergehende Anpassung an Ihre Anforderungen wünschen, können Sie die Regeln zunächst mit dem Regelassistenten definieren und anschließend manuell modifizieren.

Der Regelassistent von VirusBarrier X6 führt Sie durch mehrere Schritte zur Definition einer Regel:

- **Einführung**
- **Name und Verhalten**
- **Richtung**
- **Dienst**
- **Optionen**
- **Beenden**

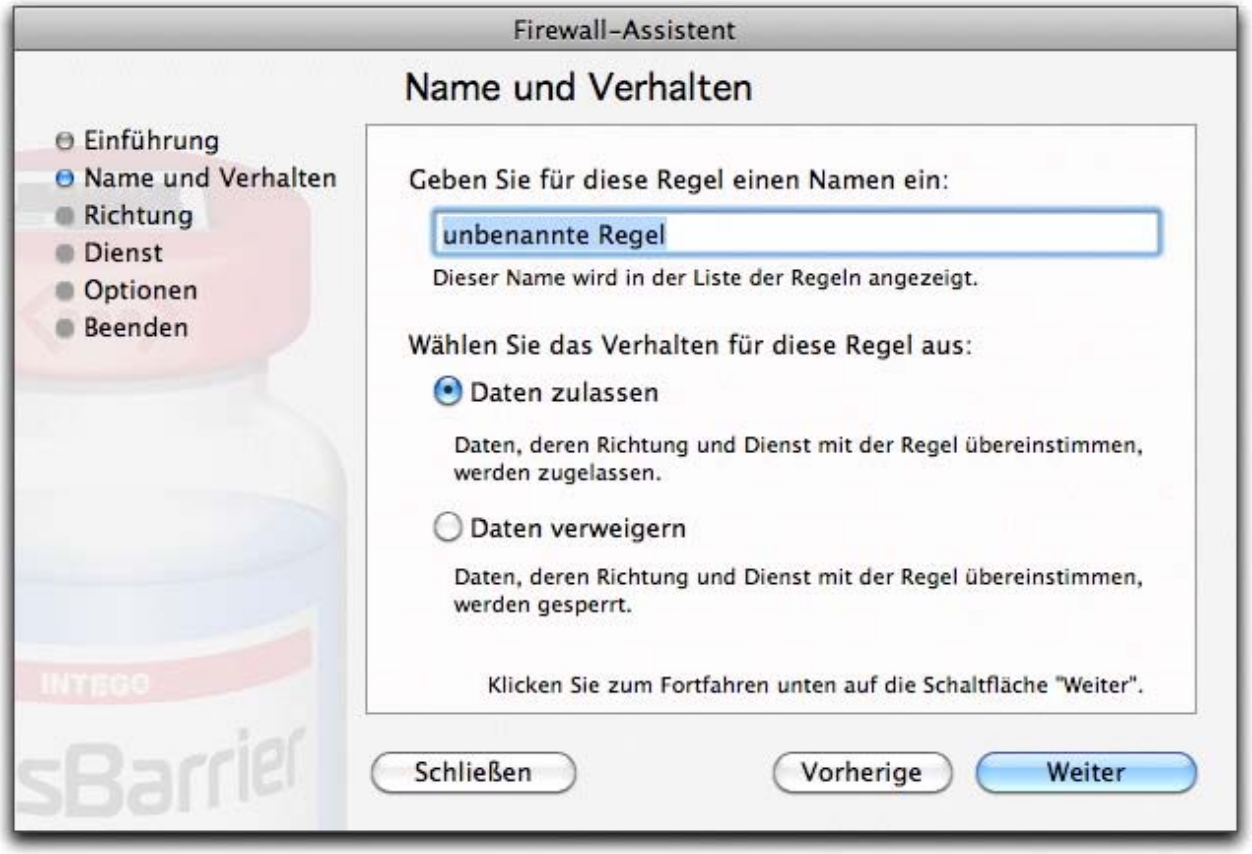
Wenn Sie eine neue Regel definieren wollen, müssen Sie auf die Schaltfläche "Assistent" klicken.



Hierauf wird das erste Dialogfeld des Regelassistenten geöffnet.

Klicken Sie auf die Schaltfläche "Weiter", um mit dem Erstellen der Regel zu beginnen. Sie können jederzeit auf die Schaltfläche "Zurück" klicken, um zu den vorherigen Fenstern zurückzukehren. Wenn Sie auf "Schließen" klicken, wird der Assistent beendet.

Name und Verhalten

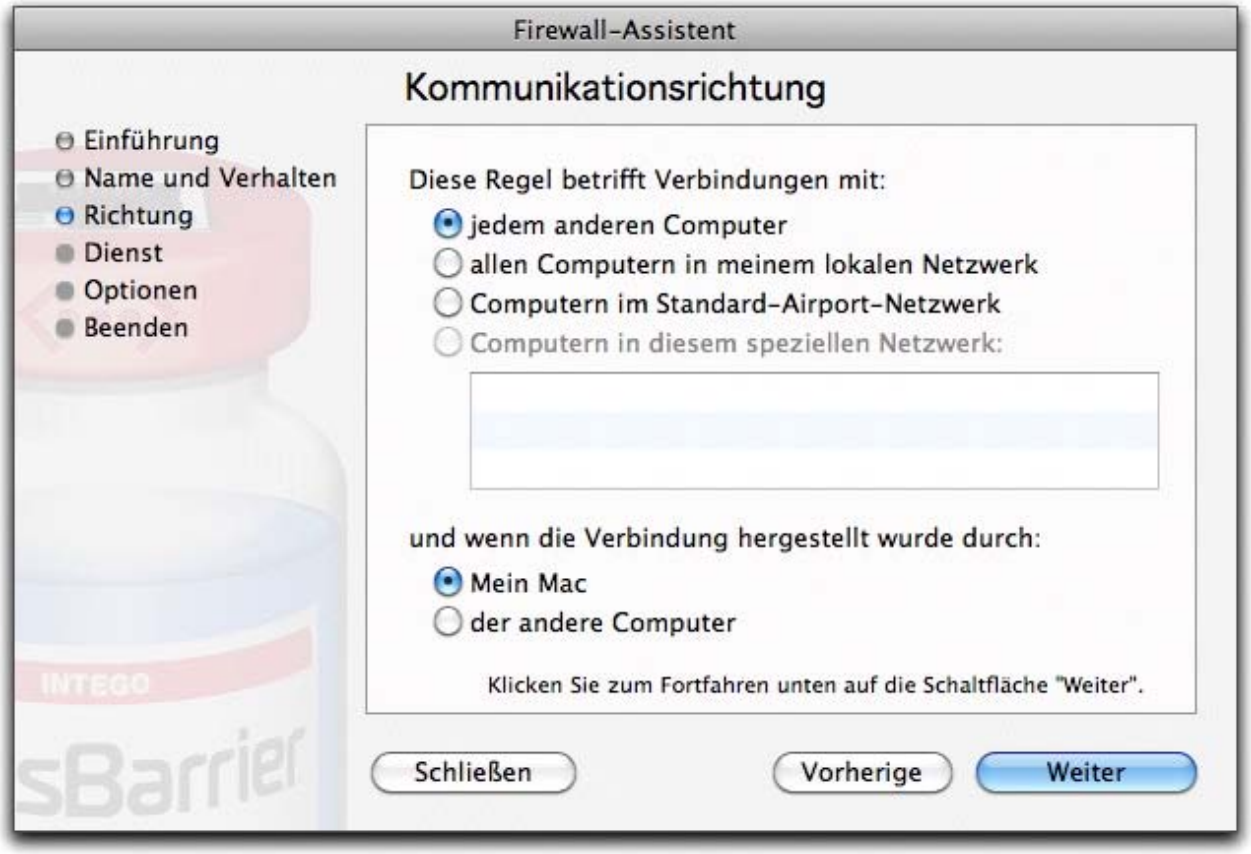


Geben Sie einen Namen in das entsprechende Feld ein und wählen Sie das Verhalten der neuen Regel: "Daten erlauben" oder "Daten ablehnen". Wenn Sie die Option "Daten erlauben" gewählt haben, gibt die Regel die Daten gemäß Transportrichtung und Dienst frei. Wenn Sie die Option "Daten ablehnen" gewählt haben, sperrt die Regel die Daten gemäß Transportrichtung und Dienst.

Klicken Sie auf die Schaltfläche "Weiter", um das nächste Fenster zu öffnen.

Kommunikationsrichtung

In diesem Dialogfeld können Sie die Richtung des Datentransfers und den Computer wählen, von dem die Verbindung hergestellt wird.



Wählen Sie zuerst im Abschnitt **Diese Regel wirkt sich auf Verbindungen aus mit:** einen Remote-Server aus. Für die Auswahl des Remote-Servers bestehen vier Möglichkeiten:

- **Jedem anderen Computer**: Hierbei handelt es sich um jeden anderen Computer, der nicht Ihr Mac ist.
- **Computern in meinem lokalen Netzwerk**: Hierbei handelt es sich um jeden anderen Computer im gleichen Netzwerk, mit dem auch Ihr Mac verbunden ist.
- **Computern im standardmäßigen Airport-Netzwerk**: Hierbei handelt es sich um jeden Computer, der mit Ihrem standardmäßigen AirPort-Netzwerk (sofern vorhanden) verbunden ist.
- **Computern in diesem speziellen Netzwerk**: Wenn Sie mit dem Regelassistenten ein spezielles Netzwerk definiert haben, können Sie dieses Netzwerk wählen.

Wählen Sie nun den Computer, von dem die Verbindung hergestellt wird:

- **Mein Mac**: Der Computer, der diese Regel verwendet.
- **Der andere Computer**: Hierbei handelt es sich um den Remote-Server, den Sie im ersten Abschnitt dieses Dialogfelds definiert haben.

Klicken Sie abschließend auf die Schaltfläche "Weiter", um das nächste Fenster zu öffnen.

Dienst

In diesem Dialogfeld können Sie den Dienst wählen, auf den sich die Regel auswirkt.

Drei Arten von Diensten stehen Ihnen zur Auswahl:

- **Alle Dienste**: Alle Netzwerk-Dienste.
- **TCP-Dienste (Verbindungsdienste)**: Dienste, die eine bestehende Verbindung zwischen zwei Computern erfordern, also die Dienste HTTP, FTP, Telnet, SSH, POP3, AppleShare, usw. Dies betrifft alle TCP-Verbindungen.
- **Dieser Dienst**: Sie haben die Auswahl aus mehreren Diensten für populäre Anwendungsprogramme und Internet-Datenübertragungsprotokolle. Klicken Sie auf den Namen des gewünschten Dienstes in der Liste.

Klicken Sie abschließend auf die Schaltfläche "Weiter", um das nächste Fenster zu öffnen.

Optionen

In diesem Fenster können Sie zusätzliche Optionen für Ihre neue Regel wählen.

Firewall-Assistent
Optionen
Einführung
Name und Verhalten
Richtung
Dienst
Optionen
Beenden
Wählen Sie zusätzliche Optionen für diese Regel:
Regelnutzung protokollieren
Wenn die Datenpakete der Regel entsprechen, zeichnet die Firewall dies in ihrem Protokoll auf und zeigt so an, dass die Regel beim Filtern des Datenpakets angewandt wurde.
Die Regel außer Kraft setzen
Die Regel wird erstellt, von der Firewall aber erst nach Ihrer Freigabe verwendet.
Klicken Sie zum Fortfahren unten auf die Schaltfläche "Weiter".
Schließen
Vorherige
Weiter

In diesem Dialogfeld werden zwei Optionen zur Auswahl angeboten:

- **Regelnutzung protokollieren**: Die Firewall speichert jedes Mal, wenn diese Regel angewendet wurde, im Protokoll.
- **Die Regel außer Kraft setzen**: VirusBarrier X6 erstellt die Regel zwar, deaktiviert sie jedoch. Sie können die Regel manuell aktivieren.

Klicken Sie abschließend auf die Schaltfläche "Weiter", um das nächste Fenster zu öffnen.

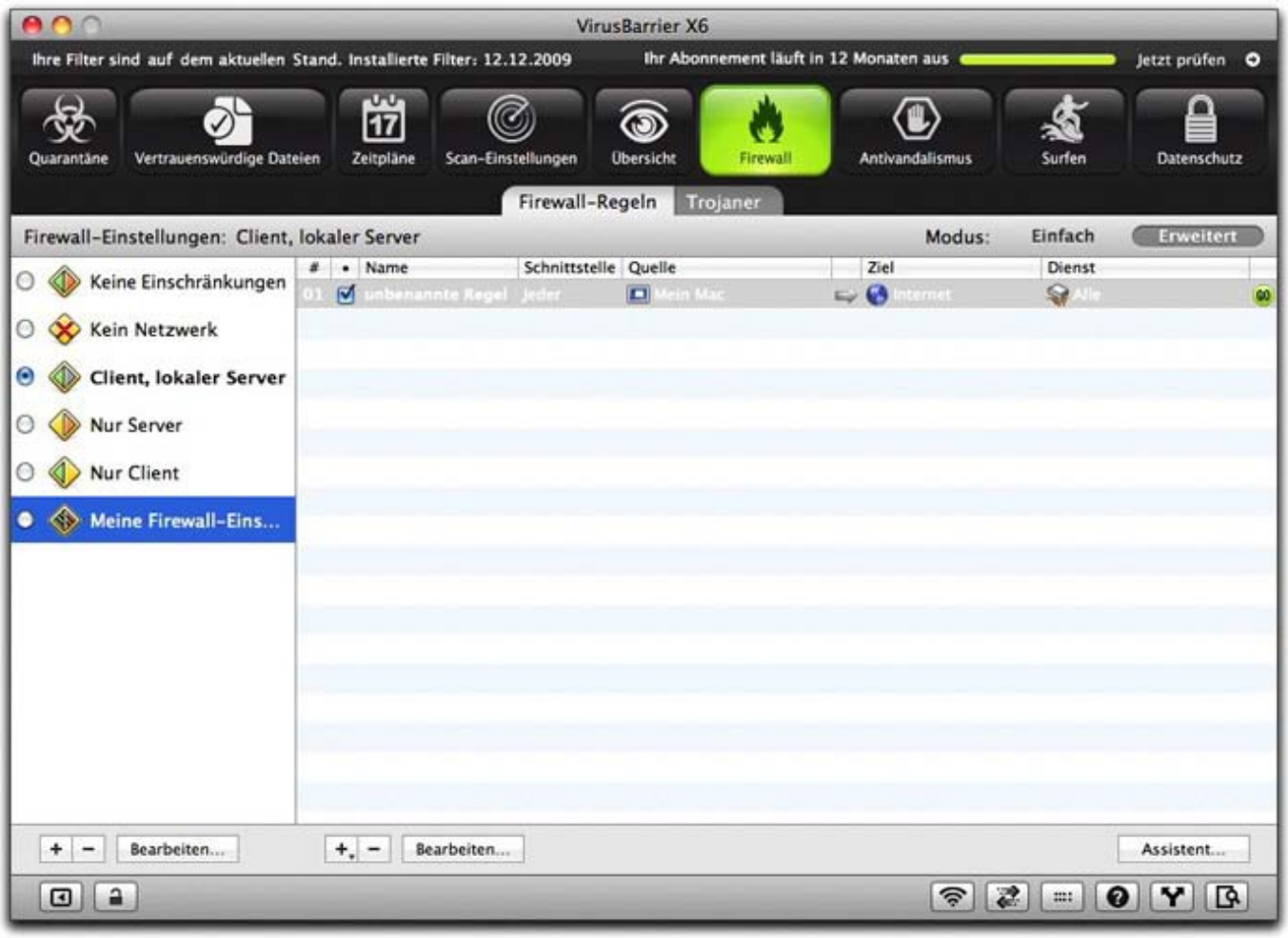
Beenden

In diesem Dialogfeld wird das Erstellen der Regel gemäß den mit dem Regelassistenten vorgenommenen Einstellungen bestätigt.

In diesem Dialogfeld wird nur eine einzige Option zur Auswahl angeboten: Wenn Sie das Kontrollkästchen **Regel für die Datenübertragung in Gegenrichtung erstellen** markieren, erstellt der Regelassistent eine übereinstimmende Regel, bei der Datenquelle und Datenziel vertauscht sind.

Klicken Sie auf die Schaltfläche "Konfigurieren", um eine neue Regel zu definieren und den Regelassistenten zu beenden.

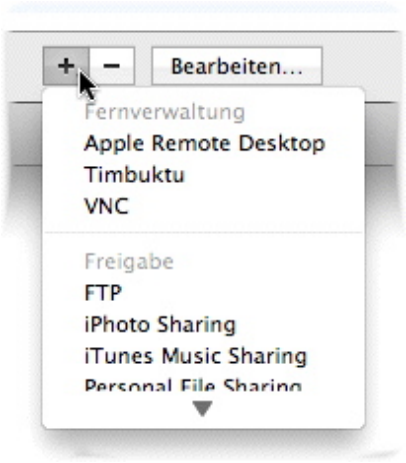
Nach dem Erstellen der Regel werden Sie sehen, dass die Regel bzw. Regeln (wenn Sie das Kontrollkästchen **Regel für die Datenübertragung in Gegenrichtung erstellen** markiert haben) in der Liste der Firewall-Regeln angezeigt wird bzw. werden.



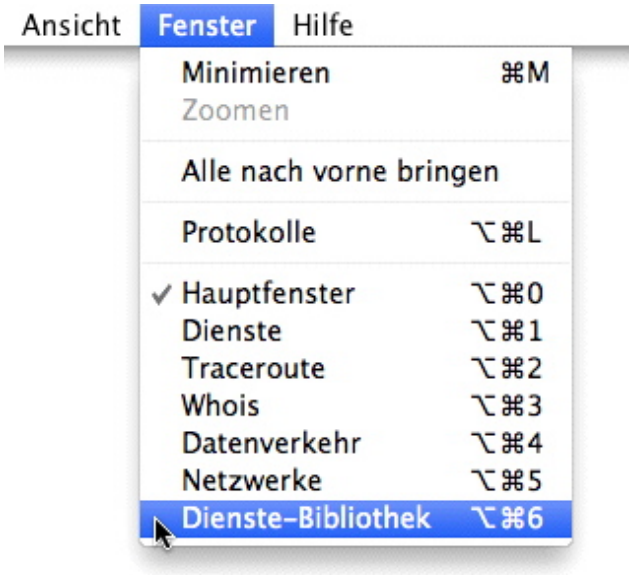
Wenn Sie die Regel modifizieren wollen, gehen Sie bitte gemäß dem Unterabschnitt "Ändern von Regeln" weiter unten vor.

So erstellen Sie Dienste-spezifische Regeln schnell

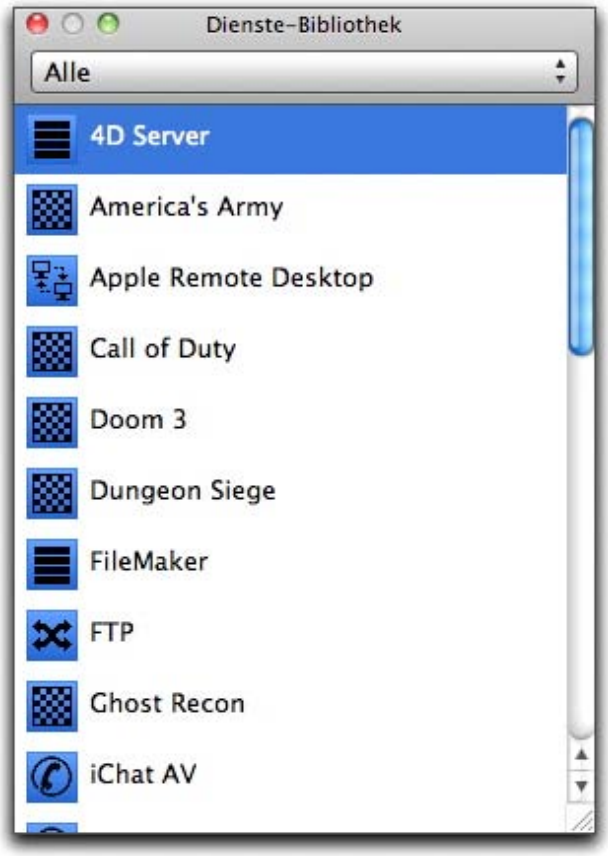
Sie können auf zwei verschiedene Arten schnell Regeln erstellen, um den Informationsfluss zu und von bekannten Diensten und Programmen zu kontrollieren. Klicken Sie entweder auf die Schaltfläche "+" unterhalb der Regelliste und halten Sie Ihre Maustaste eine Sekunde lang gedrückt. Sie können dann in einer Popup-Liste aus den am häufigsten gebrauchten Diensten wählen. Dann wird eine Regel, die Ihre Auswahl verwaltet, in der Regelliste angezeigt.



Oder Sie erstellen Dienste-spezifische Regeln schnell mit der Dienste-Bibliothek. Wählen Sie "Fenster > Dienste-Bibliothek" oder drücken Sie Wahltaste-Befehlstaste-6, um sich die Dienste-Bibliothek anzeigen zu lassen.



Das Fenster für die Dienste-Bibliothek wird daraufhin geöffnet und zeigt eine Liste der am häufigsten verwendeten Dienste an.



Wenn Sie eine neue Regel erstellen möchten, wählen Sie den gewünschten Dienst aus und ziehen Sie ihn in die Regelliste. Standardmäßig erlauben auf diese Weise hinzugefügte Regeln jeden Datenverkehr von Ihrem Mac zum Internet, über alle Schnittstellen. Anders gesagt: Die Regel verbietet keinerlei Aktivität, solange Sie die Einstellungen nicht wie zuvor beschrieben bearbeitet haben.

So erstellen Sie Regeln manuell

Mit dem Regel-Editor können Sie individuelle Regeln erstellen. Klicken Sie auf die Schaltfläche "+" unterhalb der Regelliste. Daraufhin wird Ihnen der Regel-Editor angezeigt.

Mit dem Regel-Editor von VirusBarrier X6 können Netzwerkadministratoren schnell und einfach eine umfassende Sicherheitsrichtlinie festlegen und anwenden. Der Editor ist extrem flexibel und Sie können innerhalb von Sekunden eine unbegrenzte Anzahl von Regeln erstellen. Zum Erstellen einer Regel müssen Sie Einzelheiten in sechs Bereichen festlegen:

- **Regelbenennung, Protokollierung, Auswertung und Zeitpläne**
- **Regelquelle**
- **Regelziel**
- **Regeldienst**
- **Regelschnittstelle**
- **Regelaktion**

Regelbenennung, Protokollierung, Auswertung und Zeitpläne

Am oberen Rand des Regel-Editors befindet sich ein Textfeld, in das Sie den Namen der Regel eingeben können.

Direkt darunter befindet sich das Kontrollkästchen für das Protokoll. Wenn Sie das Kästchen für das Protokoll markieren, wir jedes Mal, wenn diese Regel aktiv wird, ein Eintrag in das Protokoll von VirusBarrier X6 geschrieben. Ein kleiner roter Punkt rechts neben dem Namen der Regel in der Regelliste zeigt an, dass die Regel protokolliert wird. Wenn dieses Kontrollkästchen nicht markiert ist, wird diese Regel nicht protokolliert.

Wenn das Kontrollkästchen für das Protokoll markiert ist, steht das Kontrollkästchen "Auswerten der Regeln anhalten" zur Verfügung und ist standardmäßig markiert. Diese beiden Einstellungen bieten zusammen eine leistungsstarke Möglichkeit, um Probleme in einem Netzwerk zu beheben, ohne den Datenverkehr zu behindern.

ACHTUNG: Wenn Sie nicht herausfinden können, warum einige Ihrer Regeln keine Auswirkungen haben, sehen Sie sich die Regeln darüber an und überprüfen Sie, ob das Kontrollkästchen "Auswerten der Regeln anhalten" für jede dieser Regeln deaktiviert ist.

Klicken Sie zum Bearbeiten des Zeitplans auf die Schaltfläche "Bearbeiten...". Hierauf wird das Fenster "Planen" geöffnet.

Der Regelstatus ist standardmäßig auf "Aktiviert" eingestellt. Das heißt, Ihre Regel ist eingeschaltet. Wenn Sie den Status auf "Abgeschaltet" einstellen, wendet VirusBarrier X6 diese Regel nicht an. Das Kontrollkästchen "Aktiviert" ermöglicht es auch, bestimmte Regeln in eine Konfiguration aufzunehmen, aus anderen aber auszuschließen. Weitere Informationen über das Verwenden von Konfigurationen finden Sie im Kapitel 6, Einstellungen und Konfigurationen.

Wenn Ihr Regelstatus standardmäßig eingeschaltet ist, können Sie bestimmte Zeitpunkte festlegen, an denen die Regel ausgeschaltet wird. Wenn Ihr Regelstatus standardmäßig ausgeschaltet ist, können Sie bestimmte Zeitpunkte festlegen, an denen die Regel eingeschaltet wird.

Wenn Sie erstmals eine Regel erstellen, ist diese Regel immer aktiv. Wenn Sie die Regel für bestimmte Zeitpunkte ein- oder ausschalten möchten, klicken Sie entweder auf das Popup-Menü für "Regel aktivieren" oder "Regel ausschalten". Je nachdem, welchen standardmäßigen Regelstatus Sie gewählt haben. Wählen Sie dann einen der Zeitintervalle aus der Liste.

Außer der Option "Nie" werden noch drei weitere Optionen angeboten.

- Wenn Sie "Jede Woche" wählen, können Sie den Zeitplan der Regel so ändern, dass Sie zu einem bestimmten Zeitpunkt jede Woche eingeschaltet wird, z.B. jeden Montag um 8.00 Uhr.
- Wenn Sie "Jeden Tag" wählen, wird die Regel jeden Tag zu einem bestimmten Zeitpunkt eingeschaltet.
- Wenn Sie "Von" wählen, können Sie die Regel für einen bestimmten Zeitraum mit einer bestimmten Anfangs- und Endzeit ein- oder ausschalten.

Sie können zusätzliche Zeitpunkte zum Ein- und Ausschalten der Regeln hinzufügen, indem Sie die Schaltfläche "+" verwenden. Wenn Sie beispielsweise möchten, dass eine Regel nur montags und dienstags ausgeschaltet werden soll, können Sie diese beiden Tagen im Fenster "Planen" festlegen. Klicken Sie auf die Schaltfläche "-" rechts neben dem Element, um einen geplanten Zeitpunkt aus der Liste zu entfernen.

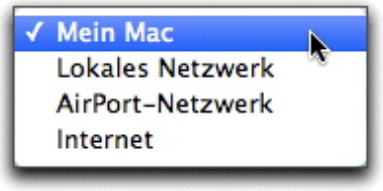
Geplante Regeln werden in der Regelliste mit einem Kalender-Symbol versehen. Für diese bestimmte Regel wurde ebenfalls die Protokollierung eingeschaltet, wie der kleine rote Punkt neben dem Namen anzeigt.

Quellen und Ziele für Regeln

Wenn Sie Regeln festlegen, ist die Quelle das Element, das die Daten sendet. Das Ziel ist das Element, an das die Daten gesendet werden. Für jede Regel können Sie aus einer Liste mit vier Quellen und Zielen wählen. VirusBarrier X6

ermöglicht es Ihnen aber nicht, für eine bestimmte Regel den gleichen Computer als Quelle und Ziel zu wählen. (Wenn Sie das versuchen, korrigiert VirusBarrier X6 den Fehler).

Standardmäßig stehen diese vier Arten von Datenquellen und -zielen zur Verfügung:



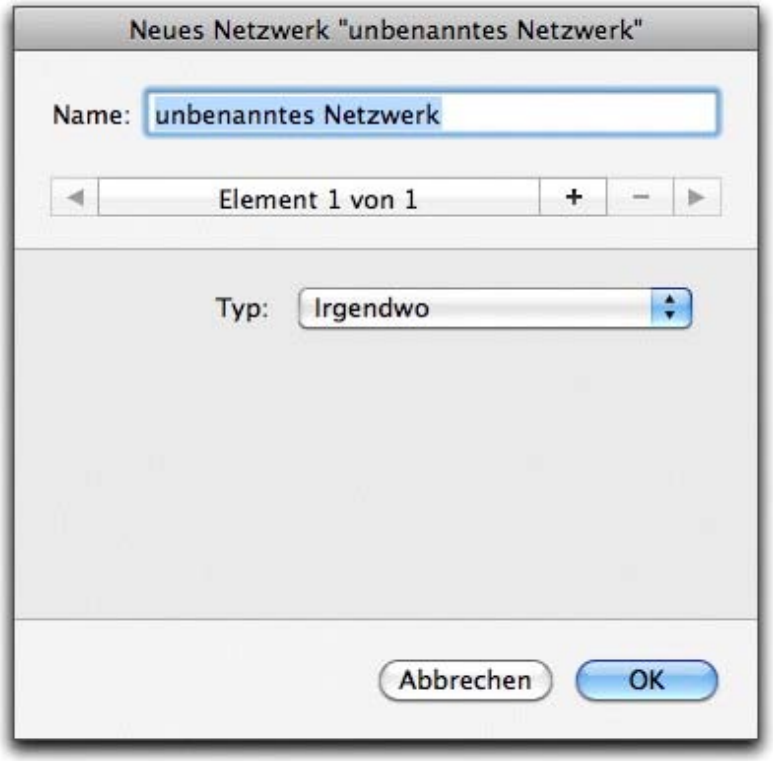
- **Mein Mac**: Ihr Computer.
- **Lokales Netzwerk**: Ein lokales Netzwerk, mit dem Ihr Computer verbunden ist.
- **Airport-Netzwerk**: Ein kabelloses AirPort-Netzwerk, mit dem Ihr Computer verbunden ist.
- **Internet**: Das Internet (zusätzlich zu jedem lokalen Netzwerk, mit dem Ihr Computer verbunden sein kann - also alle Netzwerke).

So erstellen Sie neue Quellen und Ziele

Sie können neue Datenquelle und -ziele für die Verwendung in Ihren Regeln definieren. Damit können Sie exakt angeben, mit welchen Computern Ihr Mac kommunizieren darf.

Wenn Sie eine neue Datenquelle erstellen möchten, klicken Sie auf die Schaltfläche "+" rechts neben dem Popup-Menü für Datenquellen oder -ziele. In unserem Beispiel erstellen wir eine neue Quelle. Sobald diese jedoch erstellt wurde, wird sie ebenfalls in der Liste der möglichen Ziele angezeigt.

Nun wird der Editor für neue Netzwerke geöffnet.



Geben Sie einen Namen ein, der Ihnen hilft, Sie an das Netzwerk zu erinnern. Wenn Sie beispielsweise IP-Adressen sperren, deren letzte acht Ziffern sich zwischen 100 und 155 bewegen, können Sie die Quelle/das Ziel "IPs von 100-155" nennen.

Aus einem Popup-Menü können Sie sieben verschiedene Netzwerktypen wählen.

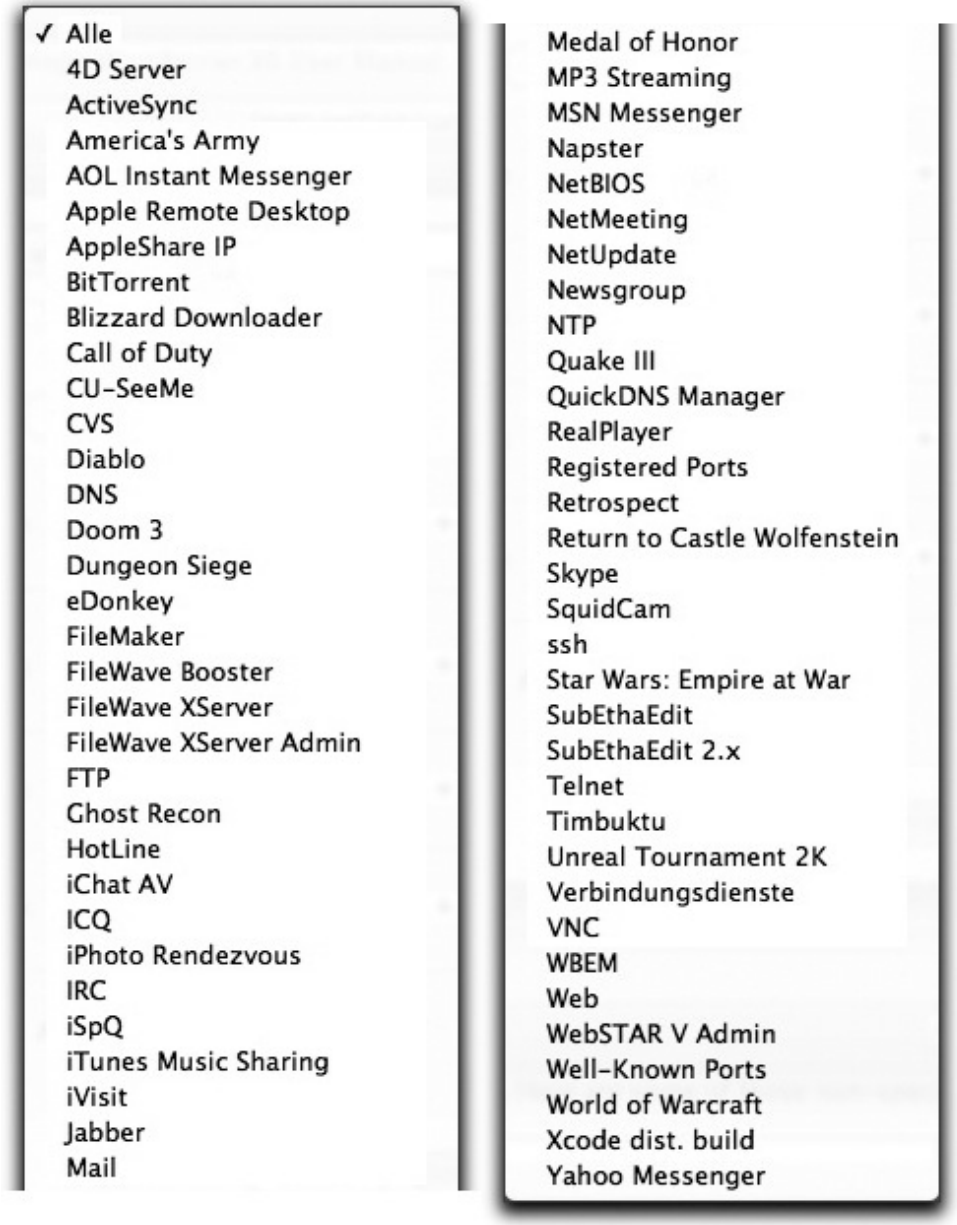
Name	Beschreibung	Adresstyp
Irgendwo	Jedes Netzwerk.	Keines, da diese Quelle alle Netzwerke abdeckt.
Mein Mac	Ihr Computer.	Die IP-Adressen von Ihrem Mac werden im Adressfeld angezeigt und können nicht geändert werden.
Mein lokales	Das lokale Netzwerk, mit dem Ihr Computer verbunden ist.	Die IP-Adressen von Ihrem Mac und die Subnet-Maske Ihres lokalen Netzwerks werden im Adressfeld angezeigt und können

Netzwerk		nicht geändert werden.
Gerät	Eine bestimmte IP-Adresse.	Jede IP-Adresse. Wenn Sie einen Domänennamen eingeben, wird dieser von VirusBarrier X6 in eine einzelne IP-Adresse aufgelöst.
Netzwerk	Ein bestimmtes Netzwerk.	Jede Subnet-IP-Adresse und Subnet-Maske. Wie im vorigen Fall löst VirusBarrier X6 Domänennamen in eine einzelne IP-Adressen auf.
Adress-Reihenfolge	Eine Gruppe von IP-Adressen.	Beginnende und endende Adressen. VirusBarrier X6 löst Domänennamen in eine einzelne IP-Adresse auf.
Ethernet-ID	Ein einzelner Computer der über Ethernet mit dem Netzwerk verbunden ist.	Eine Ethernet-ID als sechs Hexadezimal-Ziffern mit zwei Buchstaben.

Regel-Dienste

"Dienst" bezieht sich auf eine Kombination aus Protokolltyp, verwendeten Ports und Protokoll-spezifischen Kriterien. Diese Elemente beschreiben zusammen genommen üblicherweise ein Programm oder eine Programmart, das oder die Informationen sendet und empfängt. Beispielsweise wären Informationen, die per TCP-Protokoll über Port 80 unter Verwendung von HTTP gesendet werden, ein Webdienst.

Bei der Auslieferung von VirusBarrier X6 sind mehr als 50 bekannte Dienste bereits einprogrammiert. So können Sie Datenverkehr, der von einem bestimmten Typ zu sein scheint, einfach sperren (oder erlauben).



Während die meisten programmierten Dienste deutlich auf ein bestimmtes Programm abbilden, gehören einige der ausgewählten Dienste in dieser Liste, wie beispielsweise "Web", zu einer Datenübertragungsgruppe. Hier einige dieser nicht spezifischen Dienste:

Name	**Beschreibung**	**Einstellungen**
Alle	Alle Datenübertragungen, unabhängig vom Protokoll oder Port.	Alle Protokolle auf allen Ports.
Apple Remote Desktop	Ein Programm, mit dem ein Mac-Administrator andere Macs über eine Netzwerkverbindung steuern kann.	Port 3283 über UDP.
Verbindungsdienste	Alle TCP-Datenübertragungen. Eine TCP-Sitzung unterhält eine Verbindung zwischen Computern. So ist immer klar, dass	Alle TCP-Datenübertragungen auf

	sie durch einen Mac initiiert wurde und daher vertrauenswürdig ist. Eine UDP-Sitzung hingegen ist eine Reihe von Datenübertragungen von der man nicht "weiß", wer sie initiiert hat.	jedem Port.
FTP	File Transfer Protocol = Dateitransferprotokoll.	TCP, Port 20 oder 21.
iChat AV	Ein Sofortnachrichtenprogramm mit Video und Sound.	Port 5060 über UDP.
IRC	Internet Relay Chat = Internet-Relaisdialog.	TCP auf Port 194 für IRC und jeder TCP-Datenverkehr zwischen den Ports 6665 und 6669, inklusive.
iTunes Music Sharing	Eine Möglichkeit, Ihre Musikbibliothek aus iTunes über ein lokales Netzwerk mit anderen gemeinsam zu verwenden.	Port 3689 über TCP.
Mail	E-Mail-Datenübertragung.	TCP Port 25 für SMTP, Port 110 für POP3, Port 143 für IMAP4, Port 220 für IMAP3, Port 389 für LDAP und Port 587 für die Nachrichtenübertragung.
NTP	Network Time Protocol = Netzwerk-Zeitprotokoll.	UDP auf Port 123.
SSH	Secure Shell.	TCP auf Port 22 unter Verwendung von SSH.
Telnet	Remote-Anmeldung.	TCP auf Port 23 unter Verwendung von Telnet.
VNC	Virtual Network Computing, ein grafisches Remote-Kontrollsystem.	TCP auf Ports 5900-5999.
Web	Webbrowsen, beispielsweise über einen Browser wie Safari.	TCP auf den Ports 80 und 8080 über HTTP und auf Port 443 über HTTPS.
Well-Known Ports	Eine große Auswahl an Ports mit einer langen	TCP und UDP auf allen Ports

= **Bekannte Ports**	Verwendungstradition bei Netzwerk-Datenübertragungen.	von 0 bis 1023.

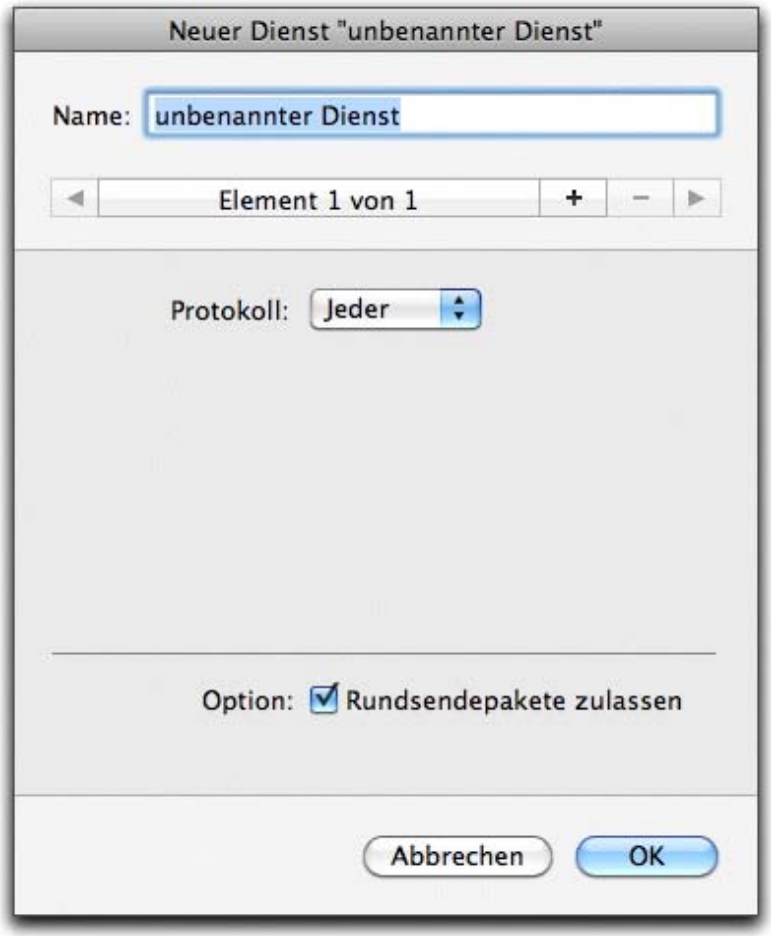
Die restlichen Dienste sind nur für bestimmte Anwendungsprogramme oder Protokolle relevant.

Gehen Sie beim Definieren von Regeln für bestimmte Dienste vorsichtig vor. Wenn Sie einen Dienst für ein bestimmtes Programm wählen, kann es vorkommen, dass dieses Programm den gleichen Port wie ein anderes Programm oder ein anderer Dienst verwendet. Durch das Sperren oder Freigeben eines Dienstes kann ein Konflikt mit anderen, allgemeineren Regeln entstehen. Wenn Sie beispielsweise ICQ-Datenverkehr sperren wollen, wird durch die Auswahl des Dienstes ICQ auch der Datenverkehr mit Hilfe des Programms "AOL Instant Messenger" gesperrt, da diese beiden Programme den gleichen Port verwenden. Andere Programme verwenden unter Umständen ebenfalls die gleichen Ports gemeinsam. Wenn Sie erkennen, dass Sie keine Verbindung mit einem bestimmten Dienst herstellen oder keine Datenpakete senden oder empfangen können, sollten Sie die von Ihnen selbst definierten Regeln nacheinander außer Kraft setzen, um zu sehen, ob hier ein Konflikt besteht.

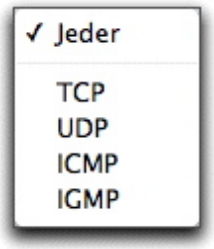
Definieren neuer Dienste

Um einen neuen Dienst zu definieren, klicken Sie im Abschnitt "Dienst" auf das Pluszeichen (+).

Nun wird der Editor für neue Dienste geöffnet.



Aus dem Popup-Menü "Protokoll" können Sie vier unterschiedliche Protokollgruppen wählen: TCP, UDP, ICMP und IGMP. Sie können auch die Option "Alle" wählen, in die sämtliche Kommunikationsprotokolle eingeschlossen sind.



Wenn Sie eine dieser Protokollgruppen wählen, werden im unteren Teil des Fensters weitere Optionen mit einer Liste der wählbaren Dienste angezeigt. Diese Optionen ändern sich je nach dem gewählten Kommunikationsprotokoll.

Für **TCP oder UDP** gibt es die folgenden Optionen:

- **Jeder Port**: Betrifft alle Ports.
- **Einzel-Port**: Sie können einen einzelnen Port festlegen. Entweder indem Sie die Port-Nummer eingeben oder indem Sie den Port aus mehr als Hundert Optionen im Popup-Menü auswählen. (VirusBarrier X6 gibt die richtige Nummer automatisch ein, wenn Sie den Port aus dem Popup-Menü wählen).
- **Reihe von Ports**: Sie können einen Bereich festlegen, indem Sie die Nummer des Anfangs- und des End-Ports eingeben.

Für **ICMP oder IGMP** gibt es die folgenden Optionen:

- **Alle**: Betrifft alle Arten.
- **Spezieller Typ**: Sie können einen einzelnen Wert festlegen. Entweder indem Sie die Nummer eingeben oder indem Sie eine von mehr als 20 Optionen aus dem Popup-Menü wählen. (VirusBarrier X6 gibt die richtige Nummer automatisch ein, wenn Sie aus dem Popup-Menü wählen). Sie können auch eine Code-Nummer festlegen, wenn nötig.

Bei allen gibt es eine Option für das Erlauben von Rundsendepaketen. Wenn dieses Kontrollkästchen markiert ist, werden Datenpakete, die an alle Computer in einem Netzwerk gesendet werden, in diesen Dienst aufgenommen.

"Ziel-Port" ist eine letzte Option, die nur für Dienste zur Verfügung steht, die das UDP-Protokoll verwenden. Wenn diese Option markiert ist, werden Pakete entprechend der Funktion des Ziel-Ports gefiltert. Wenn diese Option nicht markiert ist, werden Pakete entsprechend der Funktion des Quell-Ports gefiltert.

Regel-Schnittstellen

Eine Schnittstelle ist die Netzwerkkarte, über die Ihr Computer mit anderen Computern kommuniziert. Hierbei kann es sich um eine Ethernet-Karte, eine AirPort-Karte (für drahtlose Kommunikation Ihres Computers) oder eine andere Art von Netzwerkschnittstelle handeln.

Sie können aus der Liste der programmierten Schnittstellen auf Ihrem Computer wählen oder Ihre eigene Netzwerkschnittstelle definieren, indem Sie auf das Pluszeichen (+) klicken.

Nun wird der Editor für neue Schnittstellen geöffnet.

Das Popup-Menü für den Typ verfügt über zwei Optionen. Die erste Option "Alle" verwendet alle verfügbaren Netzwerk-Schnittstellen. Die zweite Option "Spezieller Typ" listet die Schnittstellen auf, die für Sie zur Verfügung stehen, abhängig von der Hard- und Software Ihres Computers. Hier haben Sie noch einige weitere Optionen.

Typische Schnittstellen sind folgende:

- **Airport**: Kabelloses Netzwerk
- **Integriertes Ethernet**: Kabelschnittstelle, die üblicherweise für Netzwerkverbindungen verwendet wird.
- **Integrierte FireWire-Schnittstelle**: Schnittstelle mit Kabel, die normalerweise für Peripherie-Geräte (z.B. eine Festplatte) verwendet wird, die aber auch als Netzwerk-Schnittstelle verwendet werden kann.

Der BSD-Name und die Index-Nummer sind Kennungen, die von dem Unix-Layer von Mac OS X verwendet werden. Sie können diese manuell eingeben, wenn nötig. (Sie müssen das wahrscheinlich nicht und sollten diese Kennungen auch nicht ändern, wenn Sie nicht wissen, was das ist.) Wenn andere Schnittstellen auf Ihrem Mac vorhanden sind, steht ebenfalls die Option "Andere" zur Verfügung.

Regelaktionen

Bei Verstoß gegen eine Regel sind zwei Aktionen möglich: "Erlauben" oder "Ablehnen". Wählen Sie die gewünschte Aktion für Ihre Regel, indem Sie auf das entsprechende runde Optionsfeld an der Unterseite Regel-Editors klicken.

Klicken Sie schließlich auf "OK", wenn Sie diese Regel den Firewall-Regeln von VirusBarrier X6 hinzufügen möchten.

Mehrteilige Quellen, Ziele, Dienste und Schnittstellen

Regelquellen, -ziele, -dienste und -schnittstellen können aus mehreren Elementen bestehen. Sie können beispielsweise festlegen, dass der Datenverkehr von mehreren bestimmten IP-Adressen verboten wird, indem Sie jede einzelne separat in einer vorhandenen Quelle auflisten.

Wenn Sie eine Quelle, ein Ziel, einen Dienst oder eine Schnittstelle erstellen oder bearbeiten, wird Ihnen am oberen Fensterrand eine Leiste angezeigt, die in etwa so aussieht:

- **Ein neues Element erstellen**: Klicken Sie auf die Schaltfläche "+".
- **Zwischen den Elementen wechseln**: Klicken Sie auf die Pfeilsymbole. Beachten Sie bitte, dass der Text in der Mitte Ihnen anzeigt, wo Sie sich gerade befinden und wie viele Elemente insgesamt vorhanden sind. Wenn Sie das letzte Element erreichen, können Sie mit einem Klick auf den Rechtspfeil zum ersten zurückkehren.
- **Ein Element löschen**: Sie können ein Element nur löschen, wenn es sichtbar ist. Klicken Sie so oft auf eine der beiden Pfeiltasten, bis das gewünschte Element angezeigt wird. Klicken Sie auf die Schaltfläche "-". Bestätigen Sie dann das Löschen in dem daraufhin angezeigten Dialogfeld.

Quellen, Ziele, Dienste und Schnittstellen löschen

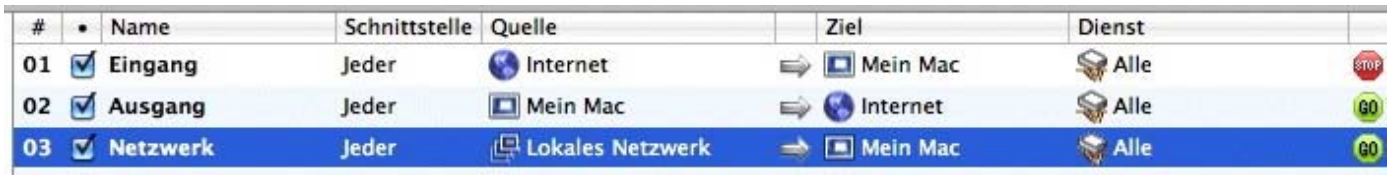
Sie können von Ihnen definierte Datenquellen löschen. Wählen Sie hierzu die zu löschende Datenquelle und klicken Sie dann auf die Schaltfläche "-".

Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie dieses Netzwerk wirklich entfernen wollen. Klicken Sie auf die Schaltfläche "Entfernen", um die Datenquelle zu löschen, und auf die Schaltfläche "Abbrechen", um sie nicht zu löschen.

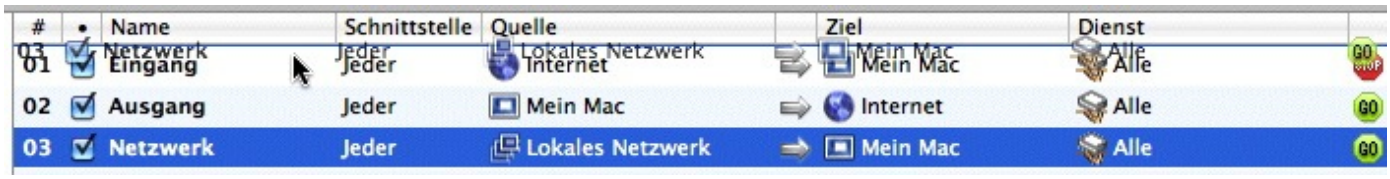
Arbeiten mit Regeln

Reihenfolge der Regeln

Die von Ihnen zur Firewall von VirusBarrier X6 hinzugefügten Regeln werden von der ersten bis zur letzten angewendet. Damit Ihre Regeln richtig funktionieren, müssen Sie also die richtige Reihenfolge haben.



Im vorstehenden Beispiel sperrt die erste Regel vom Internet eingehende Datenpakete. Hiervon sind auch Daten betroffen, die über ein anderes Netzwerk wie z.B. ein LAN (Local Area Network = lokales Netzwerk) bei Ihrem Computer eingehen. Die Regel 3 lässt Datenverkehr von einem lokalen Netzwerk zu. Da diese Regel jedoch die dritte Regel ist, wird sie nicht wirksam, da ihr die Regel 1 widerspricht. Damit die Regel 3 angewandt werden kann, muss sie in der Liste nach oben verschoben werden. Wählen Sie hierzu die Regel aus und ziehen Sie diese an die entsprechende Stelle.



Bearbeiten und Löschen von Regeln

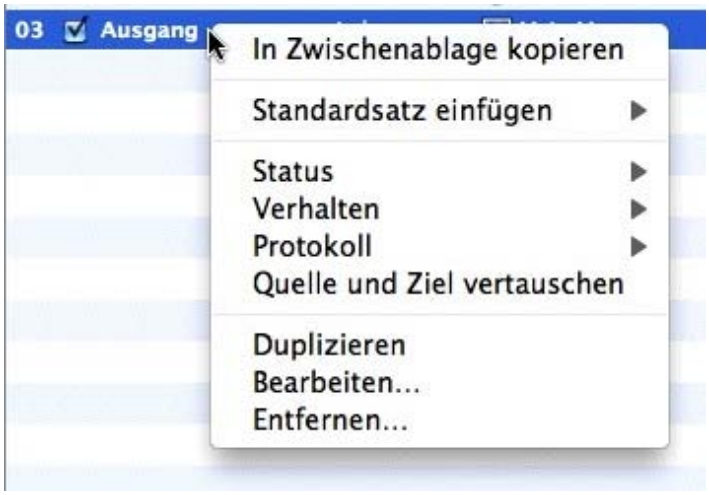
Wenn Sie eine Regel bearbeiten möchten, müssen Sie auf den Namen der Regel und dann auf die Schaltfläche mit dem Bleistiftsymbol am unteren Rand der Liste klicken. Hierauf wird der Regel-Editor geöffnet, in dem Sie alle gewünschten Änderungen an dieser Regel vornehmen können. Klicken Sie nach Abschluss der Änderungen auf die Schaltfläche "OK", um die Änderungen wirksam werden zu lassen. Wenn die Änderungen nicht wirksam werden sollen, müssen Sie auf die Schaltfläche "Abbrechen" klicken.

Wenn Sie eine Regel löschen möchten, klicken Sie auf die Regel in der Liste mit Regeln und klicken Sie dann auf die Schaltfläche "-" am unteren Rand der Liste.

So verwenden Sie das Kontextmenü für Regeln

In VirusBarrier X6 können Sie Ihre Firewall-Regeln schnell über ein Kontextmenü ändern. Sie können dieses Kontextmenü dazu verwenden, um neue Regeln hinzuzufügen, bereits definierte Regeln zu ändern und die Eigenschaften von Regeln zu ändern.

Dieses Kontextmenü wird bei gedrückter Taste "ctrl" geöffnet. Sie müssen nun nur noch auf den Namen einer Regel klicken. (Wenn Sie eine Maus mit zwei Tasten verwenden, können Sie auch auf die rechte Maustaste klicken, um das Kontextmenü zu öffnen.)



Das Menü bietet Ihnen die folgenden Optionen:

- **In Zwischenablage kopieren**: Kopiert den Inhalt einer Regel im Nur-Text-Format in die Zwischenablage des Mac. Sie können die Regel dann in ein Dokument einfügen, wo sie dann in etwa so aussieht: "#02/EIN/Eingabe/Jede/Internet -> Mein Mac/Alle/Ablehnen" (Schrägstriche stehen für Tabulatoren).
- **Standardsatz einfügen/Standardsatz hinzufügen**: Fügt einen Standardsatz von Regeln aus der gleichen Auswahl, die im einfachen Modus zur Verfügung steht, ein oder hinzu: "Keine Einschränkungen", "Kein Netzwerk", "Client, lokaler Server", "Nur Server" und "Nur Client".
- **Status**: Sie können eine Regel aktivieren oder abschalten. Wenn die Regel so geplant wurde, dass sie zu bestimmten Zeitpunkten ausgeführt wird, wird neben "Geplant" im Untermenü eine Markierung angezeigt.
- **Verhalten**: Ändert das Verhalten einer Regel von Erlauben in Ablehnen des Datenverkehrs und umgekehrt.
- **Protokoll**: Schaltet das Aufzeichnen der Datenverkehrsinformationen im Protokoll einer Regel ein und aus.
- **Quelle & Ziel vertauschen**: "Kehrt" eine Regel "um", indem die Quelle und das Ziel ausgetauscht werden.
- **Duplizieren**: Legt eine neue Kopie der Regel an.
- **Bearbeiten...**: Öffnet den Regel-Editor für die markierte Regel.
- **Entfernen...**: Löscht die Regel.

© 2009 Intego. Alle Rechte vorbehalten.